(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－313488

(43)公開日　平成10年(1998)11月24日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ
Ｈ０４Ｂ　7/15		7/15	Ｚ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｅ
			６７５Ａ

審査請求　未請求　請求項の数12　ＯＬ　（全 16 頁）

(21)出願番号　特願平10－89028

(22)出願日　平成10年(1998)４月１日

(31)優先権主張番号　９７３０２１５８．７

(32)優先日　1997年４月１日

(33)優先権主張国　イギリス（ＧＢ）

(71)出願人　597129263
アイシーオー・サーヴィシーズ・リミテッド
イギリス・Ｗ６・９ＢＮ・ロンドン・クイーン・キャロライン・ストリート・１

(72)発明者　トーマス・ゲールケ
イギリス・ＨＡ７・３ＰＮ・ミドルセックス・スタンモア・ザ・ハイウェイ・32

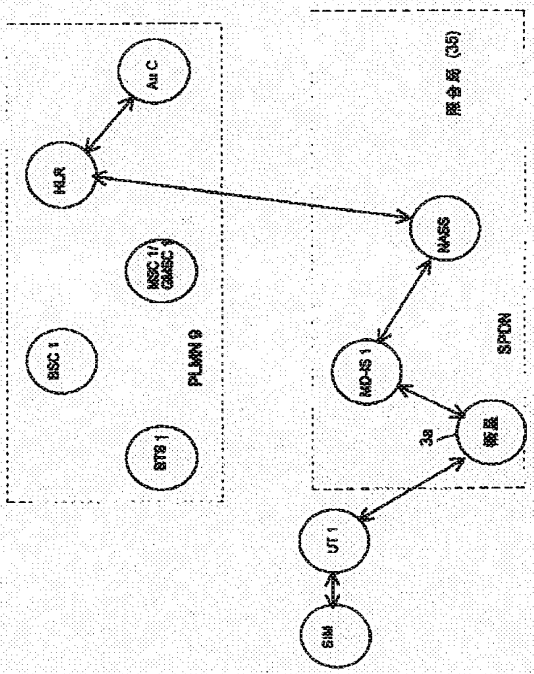
(74)代理人　弁理士　志賀　正武　（外９名）

(54)【発明の名称】　多数の遠距離通信ネットワークのためのユーザー認証方法およびシステム

(57)【要約】

【課題】　音声チャンネル通信が、ディジタルＰＬＭＮのような１つの遠距離通信ネットワークを通して行うことが可能となり、かつディジタルパケットデータ通信が、衛星ネットワークのような他のネットワークを通して行うことが可能となること。

【解決手段】　衛星遠距離通信システムにより供給された、パケットデータ通信ネットワークのための、音声チャンネルユーザー端末ＵＴ１の認証は、ユーザー端末と関連したＳＩＭカード２６からのデータ、およびユーザー端末ＵＴ１との音声チャンネル通信用に用いる従来のＧＳＭネットワーク９に関連した認証センターＡｕＣ内に保持された、対応する認証データを用いて達成される。認証データは、ＧＳＭネットワーク９から衛星パケットデータネットワークへ通信され、ネットワーク管理局ＮＡＳＳ３５内で認証が行われる。



1

【特許請求の範囲】

【請求項１】　共通の地域にサービスエリアを供給している第１または第２のモバイルネットワークを用いた使用のために移動ユーザー端末を認証する方法であって、
前記ユーザー端末が、該ユーザー端末内に保持された個々の識別コードと、遠隔の認証センターに保持された対応する識別コードとを利用する予め設定された認証手続きに従って動作可能であり、
前記ユーザー端末内に格納された前記識別コードに対応する認証データを検索するために、前記ネットワークのうちの選択された１つを通して前記認証センターにアクセスすることと、
前記認証センターから検索された前記認証データと前記ユーザー端末からのデータとを用いて、前記選択されたネットワークのために前記ユーザー端末の認証を行うこととを含むことを特徴とする移動ユーザー端末の認証方法。

【請求項２】　前記第１ネットワークが、第１のモードにおいて信号の送信をサポートし、前記第２ネットワークが、第２のモードにおいて信号の送信をサポートすることを特徴とする請求項１記載の方法。

【請求項３】前記第１モードの信号が音声チャンネル信号を含み、前記第２モードでの信号がディジタルパケットデータ信号を含むことを特徴とする請求項２記載の方法。

【請求項４】　前記第１ネットワークが衛星遠距離通信ネットワークであり、第２ネットワークがＰＬＭＮであることを特徴とする請求項１から請求項３のいずれかに記載の方法。

【請求項５】　第１モバイルネットワークを用いた使用のために移動ユーザー端末を認証する方法であって、
前記ユーザー端末が、前記第１ネットワークと共通の地域にサービスエリアを供給する第２ネットワークを用いて動作可能であり、かつ該ユーザー端末のために予め設定された認証手続きを使用し、
前記認証手続きは、前記ユーザー端末内に保持された個々の識別コードと、前記第２ネットワークの記憶位置に保持された対応する識別コードとを利用し、
前記第２ネットワーク内の前記記憶位置に保持された前記識別コードに対応する認証データを検索するために、
前記第１ネットワークから前記第２ネットワークにアクセスすることと、
前記第２ネットワークから検索された前記認証データと前記移動端末からのデータとを用いて、前記第１ネットワークにおける前記ユーザー端末の認証を行うこととを含むことを特徴とする移動ユーザー端末の認証方法。

【請求項６】　前記第１ネットワークは衛星遠距離通信ネットワークであり、前記第２ネットワークはＰＬＭＮであることを特徴とする請求項５記載の方法。

【請求項７】　ディジタルパケットデータネットワーク

2

を用いた使用のために移動ユーザー端末を認証する方法であって、
前記ユーザー端末が、音声チャンネルのための予め設定された認証手続きを用いるモバイルネットワークでの音声チャンネル通信用に動作可能であり、
前記認証手続きは、前記移動ユーザー端末内に保持された個々の識別コードと、前記音声チャンネルを供給するネットワーク内の記憶位置に保持された対応する識別コードとを利用しており、
前記音声チャンネルを供給する前記モバイルネットワーク内の前記記憶位置に格納された前記識別コードに対応する認証データを検索するために、前記ディジタルパケットデータネットワークから、前記音声チャンネルを供給する前記モバイルネットワークにアクセスすることと、
前記モバイルネットワークから検索された前記認証データと前記移動端末からのデータとを用いて、前記ディジタルパケットデータネットワーク内での前記ユーザー端末の認証を行うこととを含むことを特徴とする移動ユーザー端末の認証方法。

【請求項８】　前記ディジタルパケットデータネットワークは、前記移動ユーザー端末への衛星通信リンクを利用し、前記音声チャンネルは、地上に基地局を置く公共モバイルネットワークにより供給されることを特徴とする請求項７記載の方法。

【請求項９】　前記ユーザー端末に格納された前記識別コードに対応する識別データを、前記端末から前記ディジタルパケットデータネットワークへ送信することと、
前記認証データを前記ディジタルパケットデータネットワークから前記音声ネットワーク内の認証センターへ送信することと、
前記識別データに応じて前記認証センターから前記認証データを引き出すことと、
認証データに対応するデータについて、前記移動端末に呼びかけることと、
前記端末が前記ディジタルパケットデータネットワーク上で使用可能か否かを決定するために、前記呼びかけに応じて前記端末から引き出されたデータを前記認証データと比較することとを含むことを特徴とする請求項７または請求項８記載の方法。

【請求項１０】　前記認証データを前記ディジタルパケットデータネットワーク内の照合位置へ送信することと、
前記照合位置において、前記呼びかけに応じて前記端末から引き出された前記データを、前記認証データと比較することとを含むことを特徴とする請求項９記載の方法。

【請求項１１】　前記移動端末は、前記個々の識別コードおよび個々の識別関数を格納し、さらに前記認証センターも前記識別コードおよび前記個々の識別関数を含む

ことを特徴とする請求項９または請求項１０記載の方法。

【請求項１２】　ユーザー端末内に保持された個々の識別コードを利用する、予め設定された認証手続きに従って動作可能な移動ユーザー端末との通信のために、共通の地域にサービスエリアを供給する第１および第２のモバイルネットワークの少なくとも一部と、

前記ユーザー端末内に格納された前記識別コードに対応する認証データを含む認証センターと、

前記識別コードに対応する前記認証データを検索するために、前記第１ネットワークか前記第２ネットワークのいずれかから前記認証センターへ、前記識別コードに対応する前記ユーザー端末からのデータを送信する送信手段と、

前記認証センターから検索された前記認証データと前記ユーザー端末からのデータとを用いて、前記選択されたネットワークのために前記ユーザー端末の認証を行う認証手段とを含むことを特徴とする遠距離通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、１つ以上の遠距離通信ネットワークのための移動（mobile）ユーザー端末の認証（authenticating）に関し、かつ移動電話送受話器（handsets）のような移動ユーザー端末へ遠距離通信サービスエリア（coverage）を供給するための衛星遠距離通信ネットワークに対する、特有の、しかし限定的ではないアプリケーションを有している。

【０００２】

【従来の技術】地上の移動遠距離通信システムはよく知られており、多くの様々な規格によって動作する様々なシステムが発展してきた。これらの公共の地上モバイルネットワーク（public land mobile networks：ＰＬＭＮｓ）は、アナログあるいはディジタル規格によって動作することができる。欧州、日本を除く極東およびその他の国では、ディジタルのグローバルシステムモバイル（Global System Mobile：ＧＳＭ）ネットワークが一般的になっているのに対し、米国では、先進式移動電話システム（Advanced Mobile Phone System：ＡＭＰＳ）とディジタル式米国移動電話システム（Digital American Mobile Phone System：ＤＡＭＰＳ）とが用いられており、さらに日本では、簡易型携帯電話システム（Personal Handiphone System：ＰＨＳ）とディジタルセルラー方式（Personal Digital Cellular：ＰＤＣ）ネットワークとが用いられている。より最近では、一般移動遠距離通信システム（Universal Mobile Telecommunications System：ＵＭＴＳ）が提案されている。これらのネットワークは全てセルラー電話方式であり、地上に基地局を置く（land-based）ものである。

【０００３】例えば、ＧＳＭシステムについて考えると、モバイルネットワークの個々のセル（cell）は、一連の、地理的に離間した、地上基地送受信機局（base transceiver stations：ＢＴＳｓ）により供給されており、該ＢＴＳｓは、基地局切替センター（base switching centres：ＢＳＣｓ）を通してモバイル切替センター（mobile switching centre：ＭＳＣ）と連結されており、該ＭＳＣは、ネットワークから従来の公共切替電話ネットワーク（public switched telephone network：ＰＳＴＮ）に対してゲートウェイを供給することが可能である。前記ネットワークは、システムへの加入者およびそのユーザー端末についての情報を格納するホーム位置レジスタ（home location register：ＨＬＲ）を含む。ユーザー端末がスイッチオンされるときに、該ユーザー端末はＨＬＲに登録し、それから認証の手続きが行われる。各々の移動ユーザー端末は、加入者識別モジュール（subscriber identification module：ＳＩＭ）として知られるスマートカードを供給され、該スマートカードは、加入者を識別するために、２つの独自な識別項目を格納している。第１の項目は、国際モバイル加入者識別子（international mobile subscriber identity：ＩＭＳＩ）から構成され、第２の項目は、ＧＳＭの明細書中でＫｉとして言及された秘密パラメータから構成される。認証センター（authentication centre：ＡｕＣ）は、ＨＬＲと関連しており、ネットワークの各加入者のためのＩＭＳＩおよびＫｉに対応するデータを含む。ユーザー端末がスイッチオンされるときおよびその他のときに、ＩＭＳＩはユーザー端末からＨＬＲへ送信され、それにより、ＨＬＲはユーザーを認証するためにＡｕＣへ照会する。ＩＭＳＩは、ＡｕＣのメモリ中で照合され、対応するＫｉの値が検索される。さらに、乱数ＲＡＮＤもＡｕＣ内で発生される。該乱数ＲＡＮＤとＫｉの値は、符号付きの結果（signed result）ＳＲＥＳを発生させるために、ＧＳＭ明細書中でＡ３として言及されるアルゴリズムへの入力データとして適用される。ＡｕＣはさらに、ＧＳＭ明細書中でＡ８として言及され、秘密鍵（secret key）Ｋｃを発生させるアルゴリズムも含み、該秘密鍵Ｋｃは、ユーザー端末と地上に基地局を置くネットワークとの間で空中送信されたデータの暗号化／暗号解読のために用いられる。実際には、前記アルゴリズムＡ３／Ａ８は、うち３２ビットがＳＲＥＳを構成し、残り６４ビットがＫｃを構成するような９６ビット出力を生成させる単一のアルゴリズムにより構成されてもよい。ＲＡＮＤ、ＳＲＥＳおよびＫｃから構成される３つ組の信号は、ＡｕＣからＨＬＲを通してＭＳＣへ供給され、該ＭＳＣは、認証手続きにおいて照合局として作用する。

【０００４】そして、個々のＲＡＮＤの値は、ＭＳＣからネットワークを通ってユーザー端末へ送信される。ユーザー端末のＳＩＭは、受信された乱数ＲＡＮＤの値とＳＩＭ内に格納されたＫｉの値とから、対応するＳＲＥＳ’およびＫｃの値をユーザー端末で発生させるよう

に、局所的に格納されたアルゴリズムＡ３／Ａ８を有している。

【０００５】ＳＲＥＳ'の値は、ネットワークを通してＭＳＣへ返信され、当初に発生されたＳＲＥＳの値と比較される。これらが同じ場合、ユーザー端末は認証されるが、そうでなければユーザー端末のＨＬＲへの登録は阻止される。

【０００６】その後、ユーザー端末が認証されると、ＭＳＣは、ＧＳＭ明細書中でＡ５として言及される暗号化／暗号解読のアルゴリズムを用いて、ネットワークを通して送信されたデータの暗号化／暗号解読を開始する。該Ａ５は、その入力として、秘密鍵Ｋｃとネットワークを通して送信されたデータのフレーム番号とを用いる。ユーザー端末のＳＩＭは、局所的に格納されたアルゴリズムＡ８のコピーを用いて、それ自身の秘密鍵Ｋｃの値を発生させる。それにより、ユーザー端末での局所的なＫｃの値は、局所的に保持されたアルゴリズムＡ５のコピーを用いて、送信されたデータを暗号化／暗号解読するために用いることができる。

【０００７】ＧＳＭで用いられる認証手続きには、ユーザー端末とＢＴＳとの間の空中インタフェースで、乱数のみが送信されるという利点があり、このことは、不正登録の危険性を最小限にする。

【０００８】認証手続きおよびその後に続くデータの暗号化／暗号解読のさらなる詳細については、"The GSM System for Mobile Communications"（M.Mouly & M-B.Pautet, Cell & Sys.1992 pp 477-492）を参照のこと。

【０００９】ユーザー端末が、地理的に異なる場所の、異なるＧＳＭネットワークへ移動する場合、ユーザー端末は、訪問先のネットワークのビジター位置レジスタ（visitor location register：ＶＬＲ）に登録し、該ＶＬＲは、請求書作成発送その他の目的のために、ホーム・ネットワークであるＨＬＲと通信する。ＤＡＭＰＳ，ＰＨＳ，およびＰＤＣネットワークも、類似した位置レジスタを含んでいる。

【００１０】従来のアナログＰＬＭＮｓは、ディジタルパケットデータのサービスをサポートしてきたが、これを用いて移動ユーザー端末とファクシミリやＥメールのメッセージの送受信が可能である。例えば、ＡＭＰＳネットワークは、セルラー・ディジタル・パケット・データ（Cellular Digital Packet Data：ＣＤＰＤ）プロトコルをサポートすることができ、該プロトコルによりデータパケットを音声送信の切れ目の間に送信することが可能になる。ＣＤＰＤシステムのより詳細な説明については、"Cellular Digital Packet Data"（M.Streetharan and R.Kumar,Artech House Publishers, 1996（ISBN-0-89006-709-0））を参照のこと。しかしながら、ＤＡＭＰＳやＧＳＭのような、現行のディジタルＰＬＭＮｓは、そのようなディジタルパケットデータサービスをサポートしていないという不利を被っている。

【００１１】

【発明が解決しようとする課題】移動ユーザー端末と、ＰＳＴＮｓやＰＬＭＮｓのような従来の地上ネットワークとの間で、衛星通信リンクを用いる移動遠距離通信システムが提案されてきた。ＩＲＩＤＩＵＭ（商標）衛星セルラーシステムとして知られる１つのネットワークが、欧州特許出願公開第０３６５８８５号公報および米国特許第５，３９４，５６１号明細書（Motorola）に開示されているが、これは、いわゆる低軌道周回（low earth orbit：ＬＥＯ）衛星の立体配座（constellation）を利用しており、これらの衛星は、７８０ｋｍの軌道半径を有している。電話の送受話器のような移動ユーザー端末は、空高く軌道を描く衛星へのリンクを確立しており、通話は、該衛星から前記立体配座中の他の衛星へ送信され、それから通常は、従来の地上に基地局を置くネットワークと接続されている地上局へ送信され得る。

【００１２】いわゆる中軌道周回（medium earth orbit：ＭＥＯ）衛星の立体配座を利用する他の計画が、１０，０００～２０，０００ｋｍの範囲の軌道半径で提案されている。これについては、Walker J.G."Satellite Patterns for Continuous Multiple Whole Earth Coverage"（Royal Aircraft Establishment, pp 119-122（1977））を参照のこと。さらに、例えば、英国特許出願公開第２，２９５，２９６号公報で説明されているＩＣＯ（商標）衛星セルラーシステム、および欧州特許出願公開第０，５１０，７８９号公報で説明されているＯＤＹＳＳＥＹ（商標）衛星セルラーシステムを参照のこと。これらのシステムでは、衛星通信リンクは、隣接する衛星間での通信を許可しておらず、その代わりに、移動送受話器のような移動ユーザー端末からの信号は、最初に衛星に送信され、それから地上局あるいは衛星アクセスノード（satellite access node：ＳＡＮ）へ送信され、従来の地上に基地局を置く電話ネットワークへ接続される。これには、システムの多くの構成要素が、ＧＳＭのような既知のディジタル地上セルラー技術と互換性があるという利点がある。さらに、ＬＥＯネットワークの場合よりも簡素な衛星通信技術を用いることも可能である。

【００１３】衛星通信ネットワークにおいて、地上局は、軌道を描いて回る衛星と通信するために、世界中の様々な場所に設置されている。ＩＣＯ（商標）システムその他において、ビジター位置レジスタは、各々の衛星地上局と関連しており、該各々の衛星地上局は、特定の地上局を利用している個々のユーザー端末の記録を保持する。衛星通信ネットワークは、Ｅメール、ファックス、および他のデータの送信を可能にするために、ディジタルの衛星パケットデータネットワーク（satellite packet data network：ＳＰＤＮ）を供給すべきであるという提案がなされている。例えば、ＩＣＯ（商標）システムは、そのようなパケットデータネットワークをサ

ポートするように設計されている。

【００１４】世界のある地域では、従来の地上ＰＬＭＮおよび衛星ネットワークにより供給されたサービスエリアは、共通地域では重なり合うことになる。個々の移動端末はＰＬＭＮおよび衛星ネットワークの双方で動作可能であるべきであるという提案がなされている。ユーザー端末は、ユーザーにネットワークを選択させることを可能にするスイッチを含んでもよく、あるいはまた、例えば、信号の強度に基づいて自動選択がなされてもよい。普通は、従来の地上ネットワークが、費用や信号強度の理由で好まれることが予想される。しかしながら、あるＰＬＭＮにとっては、あるサービスをユーザー端末のために衛星ネットワークを通して供給し、他のサービスをＰＬＭＮを通して供給できれば都合がよい。例えば、ＧＳＭなどのような、ディジタルの地上に基地局を置くネットワークは、現行ではディジタルパケットデータサービスをサポートしていないので、衛星ネットワークによりデータ送信用に供給されたディジタルパケットデータのネットワークを用いるために、衛星ネットワークをＰＬＭＮの拡張として用いれば便利である。

【００１５】本発明は、例えば、音声チャンネル通信が、ディジタルＰＬＭＮのような１つの遠距離通信ネットワークを通して行うことが可能となり、かつディジタルパケットデータ通信が、衛星ネットワークのような他のネットワークを通して行うことが可能となるように、１つ以上のネットワークでの動作のための、ユーザー端末の認証に関連する。

【００１６】

【課題を解決するための手段】概して、本発明は、ユーザー端末での通信のために共通地域にサービスエリアを供給している第１または第２のモバイルネットワークで使用するための、移動ユーザー端末の認証方法を提供する。この方法では、ユーザー端末が予め設定された認証手続きに従って動作可能であり、該認証手続きは、ユーザー端末内に保持された個々の識別コードと、遠隔の認証センターに保持された対応する識別コードとを利用している。この方法は、ユーザー端末内に格納された識別コードに対応する認証データを検索するために、選択された１つのネットワークを通して認証センターにアクセスすることと、認証センターから検索された認証データとユーザー端末からのデータとを用いて、選択されたネットワークに対するユーザー端末の認証を行うこととからなっている。

【００１７】第１のネットワークが、音声信号のような第１のモードでの信号の送信をサポートし、第２のネットワークが、ディジタルパケットデータ信号のような第２のモードでの信号の送信をサポートすることも可能である。

【００１８】さらに本発明は、遠距離通信システムも提供しており、該遠距離通信システムは、ユーザー端末内に保持された個々の識別コードを利用する、予め設定された認証手続きに従って動作可能な移動ユーザー端末での通信のために、共通地域にサービスエリアを供給している第１および第２のモバイルネットワークと、ユーザー端末内に格納された識別コードに対応する認証データを含む認証センターと、識別コードに対応する認証データを検索するために、識別コードに対応するユーザー端末からのデータを、第１ネットワークまたは第２ネットワークのいずれかから前記認証センターへ送信する手段と、認証センターから検索された認証データとユーザー端末からのデータとを用いて、選択されたネットワークのためにユーザー端末の認証を行う手段とを含んでいる。

【００１９】さらに本発明は、第１モバイルネットワークでのユーザー端末通信を認証する方法も提供している。この方法では、ユーザー端末は、第１ネットワークと重なり合うサービスエリアを供給する第２モバイルネットワークで動作可能であり、かつユーザー端末のために予め設定された認証手続きを用いる。該認証手続きは、ユーザー端末内に保持された個々の識別コードと、第２ネットワークの記憶位置に保持された対応する識別コードとを利用する。前記方法は、第２ネットワークの前記記憶位置に保持された識別コードに対応する認証データを検索するために、第１ネットワークから第２ネットワークにアクセスすることと、第２ネットワークから検索された認証データと移動端末からのデータとを用いて、第１ネットワークにおけるユーザー端末の認証を行うこととからなっている。

【００２０】第１ネットワークは衛星遠距離通信ネットワークから構成され、第２ネットワークはＰＬＭＮから構成されてもよい。

【００２１】本発明は、ディジタルパケットデータネットワークを通しての通信を認証するために、音声ネットワーク用の認証手続きを利用してもよい。

【００２２】より具体的には、本発明は、ディジタルパケットデータネットワークを用いた使用のために、移動ユーザー端末を認証する方法を含み、そこでは、ユーザー端末は、モバイルネットワークを用いた音声チャンネル通信用に動作可能であり、該モバイルネットワークは、音声チャンネルのために予め設定された認証手続きを用い、該手続きは、移動端末内に保持された個々の識別コードと、音声チャンネルを供給するネットワークの記憶位置に保持された対応する識別コードとを利用する。前記方法は、音声チャンネルを供給するモバイルネットワークの前記記憶位置に格納された識別コードに対応する認証データを検索するために、ディジタルパケットデータネットワークから、音声チャンネルを供給するモバイルネットワークにアクセスすることと、モバイルネットワークから検索された認証データと移動端末からのデータとを用いて、ディジタルパケットデータネット

ワークでユーザー端末の認証を行うこととからなっている。

【００２３】ディジタルパケットデータネットワークは、移動ユーザー端末に対し、衛星通信リンクを利用してもよく、さらに音声チャンネルは、例えば、ＧＳＭネットワークのような、地上に基地局を置く公共のモバイルネットワークにより供給してもよい。

【００２４】本発明による方法は、ユーザー端末に保持された識別コードに対応する識別データを、端末からディジタルパケットデータネットワークへ送信することと、認証データをディジタルパケットデータネットワークから音声ネットワーク内の認証センターへ送信することと、識別データに応じて認証センターから認証データを引き出すことと、認証データに対応するデータを求めて、移動端末に呼びかけることと、端末がディジタルパケットデータネットワーク上で使用可能か否かを決定するために、呼びかけに応じて端末から引き出されたデータを認証データと比較することとを含んでいてもよい。

【００２５】

【発明の実施の形態】本発明がより完全に理解されるために、添付図面を参照した例により、この実施形態について以下に説明する。図１は、局所的な、地上に基地局を置く移動遠距離通信システムとともに、本発明による衛星遠距離通信システムを示す概略図である。図２は、ＳＡＮ１近傍の衛星ネットワークおよびそれに関連した地上セルラー式ネットワークのより詳細なブロック図であり、相互間の作用を示すためのものである。図３は、衛星ネットワーク内での相互通信を示す概略的なブロック図である。図４は、移動ユーザー端末の概略図である。図５は、図４で示した端末の回路の概略的なブロック図である。図６は、図４、図５で示したＳＩＭカードの概略的なブロック図である。図７は、ＧＳＭ，ＰＬＭＮ９の認証に関連したデータの流れの概略図である。図８は、ＳＰＤＮのための認証手続きの第１の実施形態の概略図である。図９は、ＳＰＤＮのための認証手続きの第２の実施形態の概略図である。図１０は、ＳＰＤＮのための認証手続きの第３の実施形態の概略図である。図１１は、認証手続きのための、ネットワーク内の様々な構成要素間でのデータ送信を概略的に示している。

【００２６】＊　衛星ネットワーク

図１を参照すると、衛星移動遠距離通信システムの概略的なブロック図が、概してＩＣＯ（商標）に対応して示されている。移動電話送受話器の形式の移動ユーザー端末ＵＴ１は、地上に基地局を置く衛星アクセスノードＳＡＮ１を用いて、地球軌道衛星３ａを経由した通信経路１，２の無線チャンネルを通して通信可能である。図１に概略的に示されているように、ＳＡＮ１には、軌道衛星を追跡できるアンテナ４が供給されている。

【００２７】多数の衛星アクセスノードＳＡＮＳ１，２，３は、共に接続されてバックボーンネットワーク５を形成しており、該バックボーンネットワーク５は、多数のゲートウェイＧＷ１，２，３を通して、従来の地上に基地局を置く電話ネットワークと接続されている。例えば、ゲートウェイＧＷ１について考えると、ＧＷ１は、地上に基地局を置く公共切替電話ネットワーク（ＰＳＴＮ）６と接続されており、該ＰＳＴＮ６は、従来の電話機７への接続を可能にする。ゲートウェイＧＷ１は、さらに公共切替データネットワーク（ＰＳＤＮ）８と公共のローカルモバイルネットワーク（ＰＬＭＮ）９とに接続されている。各々のゲートウェイＧＷ１，２，３は、ＧＳＭネットワークで用いられている型式の、商業的に入手できるモバイル切替センター（ＭＳＣ）で構成されてもよい。

【００２８】図１に示されるように、送受話器ＵＴ１は、従来の地上に基地局を置くモバイルネットワークＰＬＭＮ９で通信することもでき、該ＰＬＭＮ９は、ユーザー端末ＵＴ１との同時送受信方式のリンク１１を確立する送受信機局１０を含むように概略的に示されている。この例では、ＰＬＭＮ９は、ＧＳＭネットワークである。ＧＳＭのより完全な理解のためには、欧州遠距離通信標準協会（European Telecommunications Standard Institute：ＥＴＳＩ）により発行されている、様々なＧＳＭ勧告（GSM Recommendations）を参照のこと。さらに、より容易に理解できる概要として、前出の"The GSM System for Mobile Communications"（M.Mouly & M-B.Pautet）を参照のこと。

【００２９】衛星ネットワークは、世界的なサービスエリアを供給するように設計されており、衛星３ａ、３ｂは、衛星の立体配座の一部を形成しているが、該衛星は、いくつかの軌道に配置されてもよい。１つの例では、地表の大部分のサービスエリアを供給するように示され得る、５つの衛星を２つの軌道に配置したものが使用される。そこでは１０度の衛星の仰角に対し、１つの衛星が全ての時間に移動送受話器によってアクセスでき、２つの衛星が少なくとも８０％の時間にアクセスでき、それにより、システムの多様性を供給している。さらに冗長性（redundancy）や多様性を供給するために、さらに遠くの衛星が立体配座内に含まれてもよい。

【００３０】衛星は、通常はＭＥＯ立体配座内に、例えば１０，３５５ｋｍの軌道半径で配置されるが、本発明は、特定の軌道半径に制限されるものではない。この実施形態では、衛星３ａ，３ｂは共通の軌道内に示され、これらの衛星は、各ＳＡＮのアンテナ配列により追跡される。通常は、各ＳＡＮは、立体配座内の個々の衛星を追跡するために５つのアンテナを含む。ＳＡＮは、切れ目のないサービスエリアを供給するために、地上の至る所に間隔を置いて配置されている。示した例では、ＳＡＮ１を欧州に設置し、ＳＡＮ２をアフリカに設置し、ＳＡＮ３を米国に設置し、その他のＳＡＮを他の地域に設置してもよい。図１では、ＳＡＮ２が、衛星３ｂを経由

してユーザー端末ＵＴ２と通信しているのが示されている。衛星ネットワークのさらなる詳細については、英国特許出願公開第２，２９５，２９６号公報を参照のこと。

【００３１】衛星３ａ，３ｂは、非静止軌道内にあり、概してヒューズ（Hughes）ＨＳ６０１のような従来の衛星で構成されており、また英国特許出願公開第２，２８８，９１３号公報に開示された特徴を含んでもよい。衛星３ａ、３ｂはそれぞれ、衛星下方の地上の電波受信可能域を覆っているビームの配列を発生させるために配置されており、各々のビームは、英国特許出願公開第２，２９３，７２５号公報に開示されているような、多数の異なった周波数チャンネルやタイムスロットを含んでいる。こうしてこれらのビームは、隣接するセルラーエリアを供給し、該セルラーエリアは、従来の地上に基地局を置く移動電話ネットワークのセルに対応している。前記衛星は、衛星制御センター（satellite control centre：ＳＳＣ）１２と、追跡遠隔測定および制御局（tracking telemetry and control station：ＴＴ&Ｃ）１３とによって制御され、該ＳＳＣ１２およびＴＴ&Ｃ１３は、バックボーンネットワーク５と連結されているディジタルネットワーク１５を通して、ネットワーク管理センター１４と接続されている。ＳＳＣ１２およびＴＴ&Ｃ１３は、衛星３ａ，３ｂの動作を制御するが、それは、例えば、ＮＭＣ１４によって送信されるように、送信パワーレベルやトランスポンダーの入力チューニングを設定するためである。衛星３ａ，３ｂのための遠隔測定の信号は、ＴＴ&Ｃ１３により受信され、ＳＳＣ１２により処理され、これらの衛星が正常に機能することを確実にしている。

【００３２】電話通話の間、送受話器ＵＴ１，２は、ダウンリンクチャンネルおよびアップリンクチャンネルで構成される、完全同時送受信方式のチャンネルを経由して、衛星３ａ，３ｂにより通信する。前記チャンネルは、通話開始の際に割り当てられた周波数上にＴＤＭＡタイムスロットを含む。衛星リンクは、音声通信に用いることが可能であり、さらに、例えば、ユーザー端末とＳＡＮとの間でのファクシミリ、テキストメッセージ、Ｅメール、あるいはその他のパケットデータ送信用には２．４－６４ｋｂｐｓの範囲のデータレートで、衛星ディジタルパケットデータ通信に用いることも可能である。このように、衛星ネットワークは、衛星ディジタルパケットネットワーク（satellite digital packet network：ＳＰＤＮ）をサポートしている。

【００３３】図２を参照すると、ＳＡＮ１および局所的なＰＬＭＮ９の構成が、より詳細に示されている。ＳＡＮ１は、衛星追跡のために、５台の皿形アンテナ４に連結されている地上局ＬＥＳ１からなっており、該ＬＥＳ１は、増幅器、マルチプレクサ、デマルチプレクサ、および符復号器（codecs）を有する送受信機回路を含んでいる。移動衛星切替センターＭＳＳＣ１は、ＬＥＳ１と衛星ビジター位置レジスタVLR_{SAT}１とに連結されている。ＭＳＳＣ１は、通信信号（音声およびパケットデータ）を、バックボーンネットワーク５とＬＥＳ１とに連結させて、バックボーンネットワーク５および衛星３ａを経由した同時送受信式の通信リンク１，２を通して、個々の電話通話を移動ユーザー端末ＵＴ１へ確立することを可能にする。ＭＳＳＣ１は、アンテナ４から入ってくる通信信号上のアドレスに応じて、信号をそれらの目的地まで適切に送信する。

【００３４】VLR_{SAT}１は、各々の加入者の記録、すなわち信号通信のためにＳＡＮ１を利用している各々のユーザー端末ＵＴのＩＭＳＩを保持する。

【００３５】さらに、ＳＰＤＮ周囲のパケットデータ信号の流れを制御するために、各ＳＡＮには、図２のＳＡＮ１について示されるように、移動データ中継局ＭＤ－ＩＳが設けられている。衛星ネットワーク内のディジタルパケットデータの全体的な流れは、ネットワーク管理者（administrator）ＮＡＳＳにより制御されており、該ＮＡＳＳは、図１に示されるように、ＮＭＣ１４に都合よく設置されてもよい。

【００３６】ＭＳＳＣ１は、ゲートウェイＧＷ１に接続されており、図１に示されたＰＳＤＮ８およびＰＳＴＮ６とともに、ＰＬＭＮ９に対しても出力接続を供給している。こうして、通常はパケットデータがＰＳＤＮ８とやりとりされ、音声信号がＰＬＭＮ９あるいはＰＳＴＮ６とやりとりされることになる。登録加入者の記録を保持するために、全てのＳＡＮが、それぞれのVLR_{SAT}と類似した構造になっていることが分かる。

【００３７】図３を参照すると、衛星ネットワークは、各移動ユーザー端末ＵＴに関連する記録を含む衛星ホーム位置レジスタ（HLR_{SAT}）としてこの文中で言及されるデータベース１７も含んでいる。前記記録は、端末の識別子、すなわちそのＩＭＳＩと、該ＵＴの現在の状態、すなわち、以下により詳細に説明されるように、”局所的（local）”モードで動作しているのか、”全体的（global）”モードで動作しているのかということと、該ＵＴの地理的な位置と、請求書記録その他のデータを単一の地点において収集することができるように、該ＵＴが登録されているホームＭＳＳＣと、これにより該ＵＴが衛星経由で通信している現在動作中のＳＡＮとを含んでいる。HLR_{SAT}１７は、図１に示されているＮＭＣ１４に設置されてもよく、あるいは、ＳＡＮ１，２，３などの間で分布されていてもよい。

【００３８】図１を参照すると、ＵＴ１は次の２つの別個の状態のうちの１つに登録されてもよい。２つの別個の状態は、ＵＴが１つの局所的エリアあるいは衛星ネットワークの一部を通してのみ通信することを許容される”局所的”状態と、ＵＴが広範囲での使用を提供するように、衛星モバイルネットワークのあらゆる部分を通

って通信する資格が与えられる”全体的”状態である。

【００３９】＊　ＧＳＭネットワーク（ＰＬＭＮ９）

再び図２を参照すると、ＧＳＭモバイルネットワーク９は、多数の地上に基地局を置く送受信機局ＢＴＳ１，２，３などを含み、該ＢＴＳは、それ自体よく知られている方法で、セルラー式ネットワークをサポートするために、地理的に離間されている。通常は、ＧＳＭネットワークは、国および州上に重なるサービスエリアを有しており、それゆえ衛星ネットワークの広範囲なサービスエリアと重なり合っている。ＢＴＳ１は、接続されたアンテナ１０とともに示されており、地上通信線によって基地局切替センターＢＳＣ１へ接続されており、さらに複数のＢＴＳが、それ自体よく知られている方法で、ＢＳＣ１と接続されていることが分かる。ＢＳＣ１は、モバイル切替センターＭＳＣ１と接続されており、該ＭＳＣ１は、通話をモバイルネットワークの範囲内で、さらにゲートウェイＧＭＳＣ１を通って配線１８を介して従来のＰＳＴＮへ、あるいはさらに、配線１９を介してゲートウェイＧＷ１を通り、衛星ネットワークへ送信することが可能である。このように、音声チャンネル通話は、ＧＳＭネットワークを通してＵＴ１とやりとりできる。しかしながら、ＧＳＭネットワークは、ユーザー端末ＵＴ１とのディジタルパケットデータ送受信をサポートしていない。

【００４０】地上に基地局を置くＧＳＭネットワーク９用のホーム位置レジスタＨＬＲは、ＧＭＳＣ１と連結されて供給されている。ＨＬＲは、従来の方法では、ネットワークを用いた使用のために登録されたユーザー端末のＩＭＳＩの記録と、該ＩＭＳＩに関連した加入者の詳細とを、請求書作成発送の目的で保持する。さらにＰＬＭＮ９は、ビジター位置レジスタＶＬＲも含んでおり、該ＶＬＲは、他のＧＳＭネットワークから移動してきて、一時的にネットワークに登録された加入者の記録を保持する。例えば、ＰＬＭＮ９が英国に置かれた場合、例えばドイツなどの他国のＧＳＭネットワークからの加入者は、英国に滞在中、一時的な基盤（basis）上に局所的に登録されてもよい。電話の使用情報は、従来の方法でＶＬＲからＰＳＴＮ６を経由してドイツのネットワークへ、請求書作成発送の目的で中継される。

【００４１】認証センターＡｕＣはＨＬＲと連結されている。ＡｕＣは、Ｋｉのデータベースと乱数発生器とを含んでおり、該データベースは、ＧＳＭ勧告に従うアルゴリズムＡ３／Ａ８とともに、個々の加入者のＩＭＳＩと独自に関連している。この格納データは、後程より詳細に説明するように、端末ＵＴ１のようなユーザー端末を認証するために用いられる。

【００４２】＊　移動ユーザー端末

図４および図５を参照すると、移動ユーザー端末ＵＴ１は、局所的地上セルラー電話ネットワークおよび衛星ネットワークの両方で動作するように設計されている。したがって、図２に示されている例では、移動送受話器ＵＴ１は、地上に基地局を置くＧＳＭプロトコルか、衛星ネットワークプロトコルのいずれかに従って動作することが可能になる。図４に示されているように、ユーザー端末ＵＴ１は、デュアルモード動作が可能な移動送受話器から構成されている。これには、地上に基地局を置くセルラー式ネットワーク９を用いた使用のための従来のＧＳＭ回路が、衛星ネットワークを用いた使用のための類似した回路構成部分とともに含まれている。送受話器は、マイクロフォン２０、スピーカ２１、バッテリー２２、キーパッド２３、アンテナ２４、および衛星リンク経由で、ディジタルパケットデータネットワークを通して端末に送信されたメッセージを表示するために、他の構成部品に混じって使用され得るディスプレイ２５で構成される。さらに、手で持てる装置ＵＴ１は、加入者識別モジュール（ＳＩＭ）スマートカード２６も含む。送受話器ＵＴ１の回路構成は、ブロック図形式で図５に示されている。ＳＩＭカード２６は、通常はマイクロプロセッサである制御装置２８に連結されたＳＩＭカード読取機２７内に受け入れられる。マイクロフォン２０とスピーカ２１は、符復号器２９に連結され、該符復号器２９は、アンテナ２４に接続された従来の無線インタフェース３０に連結されており、これにより、それ自体よく知られた方法で、通信信号を送受信する。

【００４３】図６に示されるように、ＳＩＭカード２６は、メモリーＭ１を含み、該メモリーＭ１は、ＳＩＭに特有な識別関数Ｋｉ、およびＧＳＭ勧告によるアルゴリズムＡ３／Ａ８およびＡ５とともに、個々のＩＭＳＩを格納する。

【００４４】＊　ネットワーク選択

前述したように、ネットワークは、多数の様々な方法で、信号強度のような要因によって自動的に、または手動式のいずれかで選択され得る。この例では、ネットワークは、キーパッド２３上のキーを用いて手動式に選択される。

【００４５】衛星ネットワークを選択するためにキーパッド２３が操作されると、制御装置２８は、符復号器２９と無線インタフェース３０とを、衛星ネットワークに適した周波数、プロトコル、および送信周波数に合わせて構成するように動作する。音声送信チャンネルは、衛星ネットワーク用に選択することが可能である。さらに、ディジタルパケットデータサービスは、例えば、米国のＡＭＰＳネットワークでこれまでに用いられているＣＤＰＤプロトコルに従うＳＰＤＮを通して選択することが可能である。こうして、衛星ネットワークが選択されると、音声チャンネルとパケットデータ通信の両方が、同時送受信方式リンク１，２を通して衛星３ａを経由して行われる。

【００４６】ＰＬＭＮ９（ＧＳＭネットワーク）が選択されると、制御装置２８は、同時送受信方式リンク１１

を通して、地上に基地局を置くＧＳＭネットワーク音声チャンネルに適した周波数で動作するように、無線インタフェース３０を設定する。しかしながらＧＳＭネットワークは、それ自体でディジタルパケットデータサービスをサポートすることはできない。

【００４７】＊　ネットワーク相互作用

再び図２を参照すると、衛星ネットワークは、ＩＣＯ（商標）システムから構成されてもよく、該ＩＣＯ（商標）システムは、従来のＧＳＭネットワーク９あるいは他の地上に基地局を置くセルラー式ネットワークを通しては利用不可能な、強化されたサービスを供給することができる。この例では、ＧＳＭネットワーク９は、それ自体でＰＤＮをサポートできない。それゆえ、ある環境においては、ＰＬＭＮ９の拡張として衛星ネットワークを用いて、それにより地上に基地局を置くモバイルネットワーク９から衛星ネットワークを通して通話を送信し、衛星ネットワークを通して追加の利用可能なサービスを利用することが望ましい。相互作用機能装置３１は、この目的のために供給され、衛星とセルラー方式の地上に基地局を置くネットワーク間でのサービス設備の完全な制御を可能にしており、これにより、衛星ネットワークを用いることで、Ｅメールおよびその他のパケットデータサービスを、ＧＳＭネットワークによりサポートすることを可能にしている。

【００４８】＊　認証手続き

前述したように、ユーザー端末ＵＴ１がスイッチオンされたとき、通信目的のために用いられるべきネットワークに登録する必要があり、認証手続きが、ユーザー端末の正当性を決定するために行われる必要がある。ＧＳＭネットワーク（ＰＬＭＮ９）に対しては、従来のＧＳＭ登録および認証手続きが行われるが、これについては、この後図７および図１１を参照してより詳細に説明する。

【００４９】本発明によれば、この従来のＧＳＭ登録手続きが、衛星パケットデータネットワークＳＰＤＮを用いた使用のために、ユーザー端末の認証を供給するように適応されることも可能である、ということが評価されてきており、そこで、ＳＰＤＮ経由で認証手続きがどのように用いられるかについての３つの例を、図８、図９、および図１０を参照し、図１１と結びつけて説明する。まず最初にＧＳＭ登録と認証手続きについて、図７を参照して説明する。

【００５０】１．ＧＳＭネットワーク（ＰＬＭＮ９）

前述したように、ユーザー端末ＵＴ１は、ＳＩＭスマートカードを含んでおり、該ＳＩＭカードは、唯一のＩＭＳＩ、唯一の識別関数ＫｉおよびＧＳＭ暗号化アルゴリズムＡ５を、ＧＳＭ勧告に応じて格納している（図６）。登録および認証手続きは、ＩＭＳＩをＧＳＭ認証センターＡｕＣへ送信することと、照合局３５においてＳＩＭからのデータを認証センターＡｕＣからのデータと比較することとを含む。従来のＧＳＭ認証手続きでは、照合局３５はＧＳＭネットワーク内に配置されており、またＭＳＣ１に配置されていてもよい。

【００５１】図７は、ＧＳＭネットワークの種々の構成要素とユーザー端末ＵＴ１との間のデータの流れを示している。認証手続きのステップは、図１１に述べられている。

【００５２】第１のステップＳ１では、ＩＭＳＩは、ＢＴＳ１、ＢＳＣ１およびＭＳＣ１を経由してＵＴ１からＨＬＲへ送信され、そこから認証センターＡｕＣへ送信される。前述したように、認証センターＡｕＣは、ＧＳＭネットワーク上での使用にあてはまる各々のＩＭＳＩと関連した識別関数Ｋｉのコピーを含む。

【００５３】ステップＳ２では、ＩＭＳＩはＡｕＣのメモリー内で照合され、対応するＫｉの値が検索される。さらに、乱数発生器（図示せず）を用いて、乱数ＲＡＮＤがＡｕＣ内で発生される。乱数ＲＡＮＤおよびＫｉの値は、ＡｕＣ内で、符号付き結果ＳＲＥＳを発生させるために、ＧＳＭアルゴリズムへの入力として適用される。さらに、ＡｕＣは、秘密鍵Ｋｃを発生させるＧＳＭアルゴリズムＡ８も含み、該秘密鍵Ｋｃは、ユーザー端末と地上に基地局を置くネットワークとの間で空中送信されたデータの暗号化／暗号解読のために用いられる。実際には、アルゴリズムＡ３／Ａ８は、うち３２ビットがＳＲＥＳを構成し、残り６４ビットがＫｃを構成するような９６ビット出力を生成させる単一のアルゴリズムで構成してもよい。

【００５４】ステップＳ３では、ＲＡＮＤ、ＳＲＥＳおよびＫｃからなる３つ組の信号が、認証センターＡｕＣからＨＬＲを通してＭＳＣへ供給され、該ＭＳＣは、認証手続きにおいて照合局３５として機能する。実際には、例えば通話中に、すぐ後の認証における使用のために、ｎ個の３つ組信号がＭＳＣへ供給されるが、ここでは説明を簡潔にするために、３つ組が１つだけの処理について考えることにする。

【００５５】ステップＳ４では、個々のＲＡＮＤの値が、ＭＳＣからネットワークを通ってユーザー端末へ送信される。ユーザー端末ＵＴ１のＳＩＭは、アルゴリズムＡ３／Ａ８を格納しており、これにより、ステップＳ５において、受信された乱数値ＲＡＮＤおよびＳＩＭ内に格納されたＫｉの値から、対応するＳＲＥＳ’の値がユーザー端末ＵＴ１で発生する。

【００５６】ＳＲＥＳ’の値は、ステップＳ６において、ネットワークを通ってＭＳＣへ返信され、ステップＳ７において、当初に発生されたＳＲＥＳの値と比較される。これらが同じ場合、ユーザー端末は認証されるが、そうでなければユーザー端末のＨＬＲへの登録は阻止される。

【００５７】認証が成功した場合、ＭＳＣは、ＧＳＭ明細書中でＡ５として言及されたアルゴリズムを用いてネ

ットワークを通して送信されたデータの暗号化／暗号解読を開始し、該Ａ５は、その入力として、秘密鍵Ｋｃ、およびネットワークを通して送信されたデータのフレーム番号とを用いる。暗号化および暗号解読は、実際にはＢＳＣあるいはＢＴＳにおいて行われる。ユーザー端末ＵＴ１のＳＩＭは、局所的に格納されたアルゴリズムＡ８のコピーを用いて、それ自身の秘密鍵Ｋｃの値を発生する。こうして、ユーザー端末ＵＴ１におけるＫｃの局所的な値は、局所的に保持されたアルゴリズムＡ５のコピーを用いて、データを暗号化／暗号解読するために用いられ得る。

【００５８】本質的な乱数のみが、空中インタフェースを通して送信されるが、該乱数どうしは互いに無関係であり、複製や認証されていない使用の危険性を最小限にするということが分かる。

【００５９】本発明によれば、以下に説明するように、この一般的な技術は、ＳＰＤＮを認証するために用いることも可能であるということが、評価されてきている。

【００６０】２．衛星ディジタルパケットネットワークの認証

２．１　第１の実施形態

図８および図１１を参照して、以下にＳＰＤＮの認証のためのデータの流れを説明する。認証手続きは、ＳＩＭからのＩＭＳＩ、およびＧＳＭネットワークＰＬＭＮ９のＡｕＣ内に保持された、Ｋｉの格納された値を利用する。手続きのステップは、概して図１１に示されたものと同様であるが、この場合、照合局３５がＮＡＳＳから構成されている。

【００６１】ステップＳ１では、ＳＰＤＮを用いた使用のためにユーザー端末ＵＴ１を認証すべく、ＩＭＳＩは、衛星３ａとＭＤ－ＩＳ１（ＳＡＮ１と関連している）を経由し、ＮＡＳＳ（ＮＭＣ１４と関連している）を経由し、そしてＧＷ１（図１）を経由して、ＰＬＭＮ９へ送信されるが、さらにＩＭＳＩは、図８に概略的に示されているように、ＨＬＲおよびＡｕＣへ送信される。それから、図７を参照して説明されているように、ステップＳ２では、ＩＭＳＩはＡｕＣのメモリー内で照合され、正当であれば、対応するＫｉの値がメモリーから引き出される。さらに、個々のＲＡＮＤの値が発生され、アルゴリズムＡ３／Ａ８がＲＡＮＤおよびＫｉに対して動作し、ＳＲＥＳとＫｃとを生成させる。

【００６２】そしてステップＳ３では、ＳＲＥＳ、Ｋｃ、およびＲＡＮＤの３つ組は、ＡｕＣから照合局３５、すなわちＮＡＳＳへ送信される。

【００６３】ステップＳ４では、個々のＲＡＮＤの値は、ネットワークを通って、衛星３ａ経由でユーザー端末ＵＴ１へ返信され、そこで、ステップＳ５では、対応するＳＲＥＳ’の値が図７を参照して前述したように発生される。ステップＳ６では、ＰＬＭＮ９のＨＬＲから以前に受信された３つ組中のＳＲＥＳの値と比較するために、発生したＳＲＥＳ’の値が、衛星３ａおよびＭＤ－ＩＳ１を経由してＮＡＳＳへ返信される。

【００６４】ステップＳ７では、ＳＲＥＳおよびＳＲＥＳ’の値が比較され、それらが同一であれば、ユーザー端末はＳＰＤＮを用いた使用のために認証される。

【００６５】こうして、図７および図８を参照して説明された手続きは、ユーザー端末をＰＬＭＮ９かＳＰＤＮのいずれかのために選択的に認証されることを可能にし、それにより、ユーザー端末は、ＧＳＭネットワーク、すなわちＰＬＭＮ９上の音声通信用および衛星３ａを経由したネットワークＳＰＤＮを通したパケットデータ通信のために用いられ得る。

【００６６】認証手続きは、送信中、例えば、システムがある通信セルから他のセルへ渡され、かつ他の（ｎ－１）個の３つ組がこの目的のために使用され得るときに、繰り返されてもよいということが分かる。

【００６７】２．２　第２の実施形態

図９を参照すると、ＳＲＥＳとＳＲＥＳ’の照合（ステップＳ７）が、図２に示された相互作用機能装置（interworking function unit）ＩＷＦで行われるように、図８に示された認証手続きが変更可能である。したがって、ＩＷＦは、照合局３５として機能する。図９は、この実施形態での使用のためのデータの流れを示す。ＳＲＥＳの値および対応するＳＲＥＳ’の値は、図８を参照して説明された（ステップＳ１－Ｓ６）のと同様の方法で生成されるが、信号値の比較（ステップＳ７）はＩＷＦで行われる。

【００６８】２．３　第３の実施形態

照合局３５の機能は、適切なＳＡＮ（図２）内のＭＳＣ１においても行われ得る。図１０を参照すると、認証手続きのための対応するデータの流れが示されている。ＳＲＥＳの値および対応するＳＲＥＳ’の値は、前述したのと同様に生成され、比較のためにＭＳＳＣ１へ送られ、それにより、ユーザー端末ＵＴ１をＳＰＤＮを用いた使用のために認証する。

【００６９】音声とパケットデータ双方の通信が、リンク１，２によって衛星ネットワークを通して完全に行われ、かつＰＬＭＮ９が選択されていない場合には、端末は、図１に示されたＨＬＲ$_{SAT}$と接続された認証センター（図示せず）によって認証される。

【００７０】他の多くの修正が、本発明の範囲内に入る。例えば、ＰＬＭＮ９は、日本でのＰＨＳ，ＰＤＣ、あるいはある欧州の国々でのＤＣＳ１８００、あるいは新たに提案されたＵＭＴＳなどの、多数の異なる規格およびプロトコル上で動作可能であることが分かる。

【００７１】また、本発明は、ＩＣＯ（商標）衛星ネットワークに関連して説明されてきたけれども、他の衛星ネットワークを、様々な立体配座および信号送信プロトコルで用いることも可能である。

【００７２】さらに、経路１，２上での信号通信がＴＤ

ＭＡアクセスプロトコルを用いるけれども、符号分割多元接続（code division multiple access）（ＣＤＭＡ）あるいは周波数分割多元接続（frequency division multiple access）（ＦＤＭＡ）のような他のプロトコルを用いることも可能である。

【００７３】説明の便宜上、ユーザー端末ＵＴを表すために”移動（mobile）”という語を用いてきたが、この語は、手に持てる、あるいは携帯用の端末に制限されるのではなく、例えば、船あるいは飛行機に、あるいは陸上の車両に搭載される端末をも含んでいることは理解されるべきである。さらに、ある端末ＵＴを完全に、あるいは少なくとも部分的に固定して、本発明を実施することも可能である。

【図面の簡単な説明】

【図１】　局所的な、地上に基地局を置く移動遠距離通信システムとともに、本発明による衛星遠距離通信システムを示す概略図である。

【図２】　ＳＡＮＩ近傍の衛星ネットワークおよびそれに関連した地上セルラー式ネットワークのより詳細なブロック図であり、相互間の作用を示すためのものである。

【図３】　衛星ネットワーク内での相互通信を示す概略的なブロック図である。

【図４】　移動ユーザー端末の概略図である。

【図５】　図４で示した端末の回路の概略的なブロック図である。

【図６】　図４、図５で示したＳＩＭカードの概略的なブロック図である。

【図７】　ＧＳＭ，ＰＬＭＮ９の認証に関連したデータの流れの概略図である。

【図８】　ＳＰＤＮのための認証手続きの第１の実施形態の概略図である。

【図９】　ＳＰＤＮのための認証手続きの第２の実施形態の概略図である。

【図１０】　ＳＰＤＮのための認証手続きの第３の実施＊形態の概略図である。

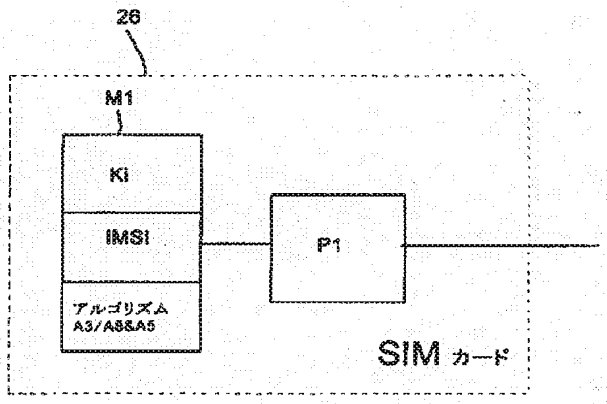
【図１１】　認証手続きのための、ネットワーク内の様々な構成要素間でのデータ送信を概略的に示している。

【符号の説明】

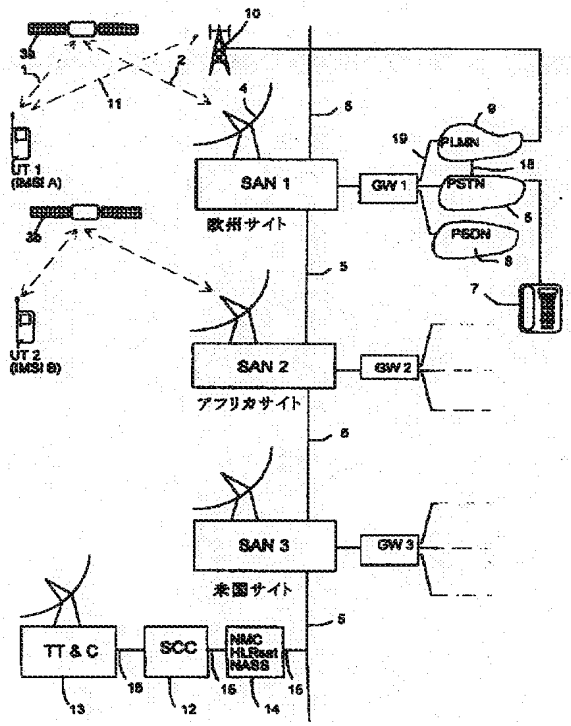
ＵＴ１，ＵＴ２　ユーザー端末
ＧＷ１，２，３　ゲートウェイ
１，２，１１　同時送受信方式リンク
３ａ，３ｂ　衛星
４　皿形アンテナ
５　バックボーンネットワーク
６　ＰＳＴＮ
７　電話機
８　ＰＳＤＮ
９　ＰＬＭＮ
１０　アンテナ
１２　ＳＣＣ
１３　ＴＣ＆Ｃ
１４　ＮＭＣ
１５　ディジタルネットワーク
１７　データベース
１８，１９　配線
２０　マイクロフォン
２１　スピーカ
２２　バッテリー
２３　キーパッド
２４　アンテナ
２５　ディスプレイ
２６　ＳＩＭスマートカード
２７　ＳＩＭカード読取機
２８　制御装置
２９　符復号器
３０　無線インタフェース
３１　相互作用機能装置（ＩＷＦ）
３５　照合局

整理番号　Ｆ０５０１７Ａ１

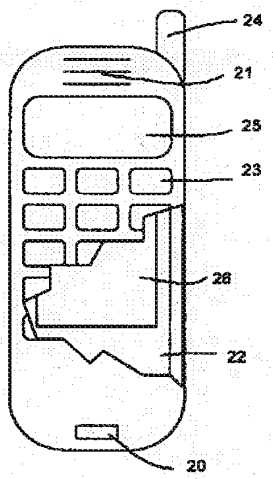
【図６】



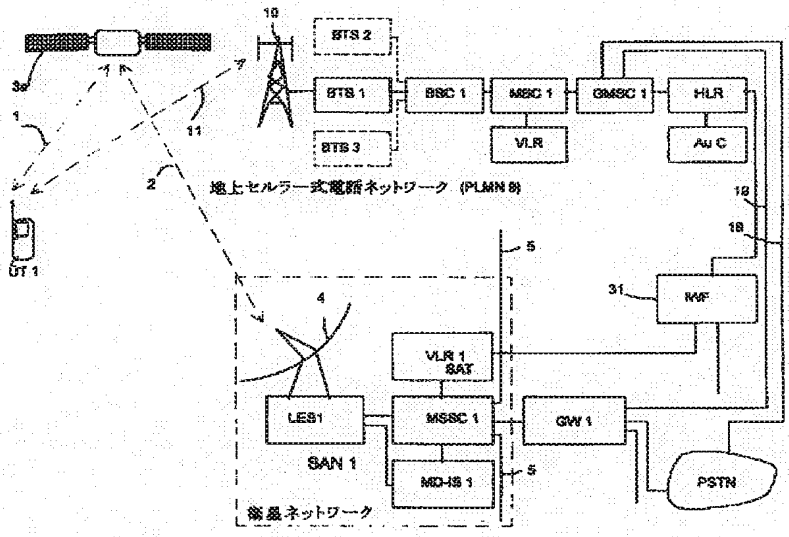
【図１】


SAN 1
欧州サイト
SAN 2
アフリカサイト
SAN 3
米国サイト
GW 1
GW 2
GW 3
PLMN
PSTN
PSDN
TT & C
SCC
NMC
HLRsat
NASS
UT 1
(IMSI A)
UT 2
(IMSI B)

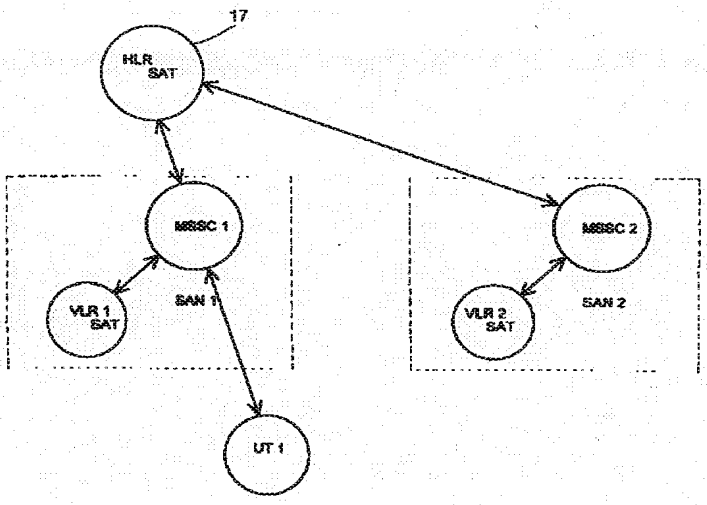
【図４】


UT 1

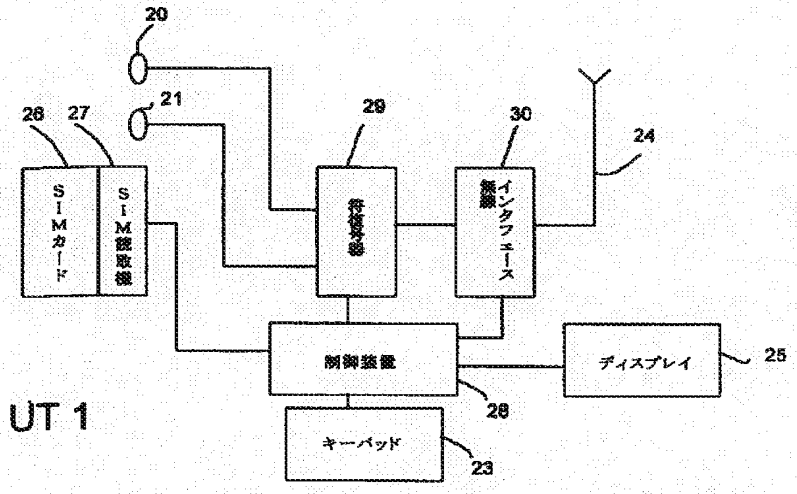
【図２】


BTS 2
BTS 1
BTS 3
BSC 1
MSC 1
GMSC 1
HLR
VLR
Au C
地上セルラー式電話ネットワーク (PLMN B)
UT 1
IWF
VLR 1
SAT
LES1
MSSC 1
GW 1
SAN 1
MD-IS 1
PSTN
衛星ネットワーク

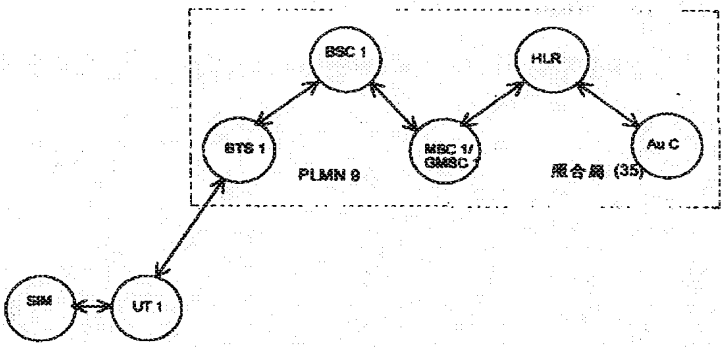
【図３】


17
HLR
SAT
MSSC 1
MSSC 2
VLR 1
SAT
SAN 1
VLR 2
SAT
SAN 2
UT 1

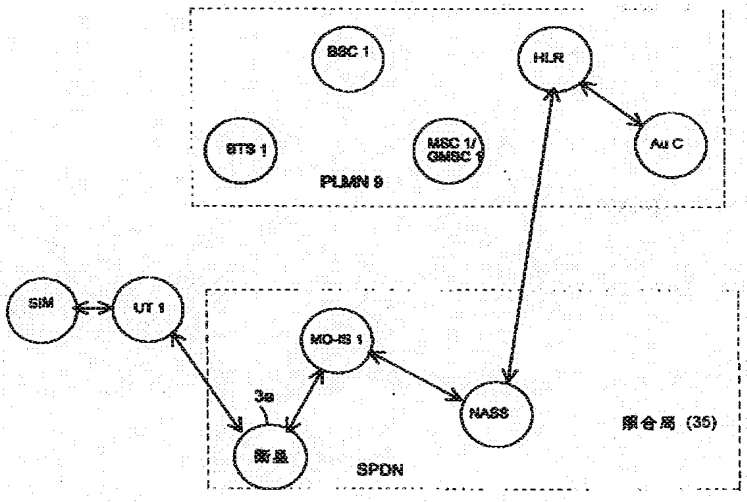
【図５】


20
21
28
27
29
30
24
SIMカード
SIM読取装置
インタフェース
制御装置
ディスプレイ
25
26
キーパッド
23
UT 1

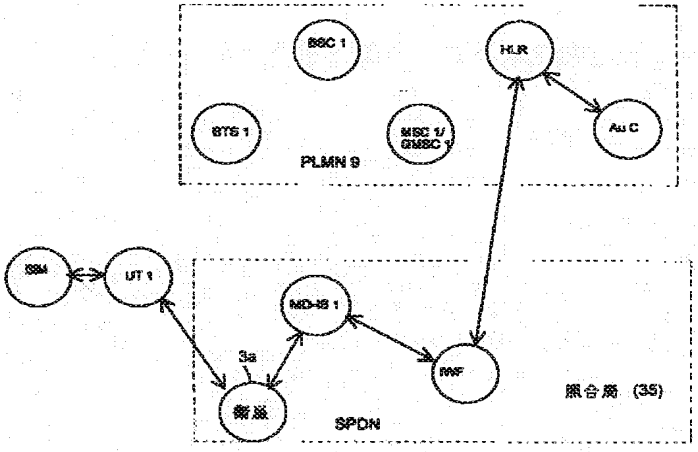
【図７】


BSC 1
HLR
BTS 1
MSC 1/
GMSC
Au C
PLMN 9
照合局 (35)
SIM
UT 1

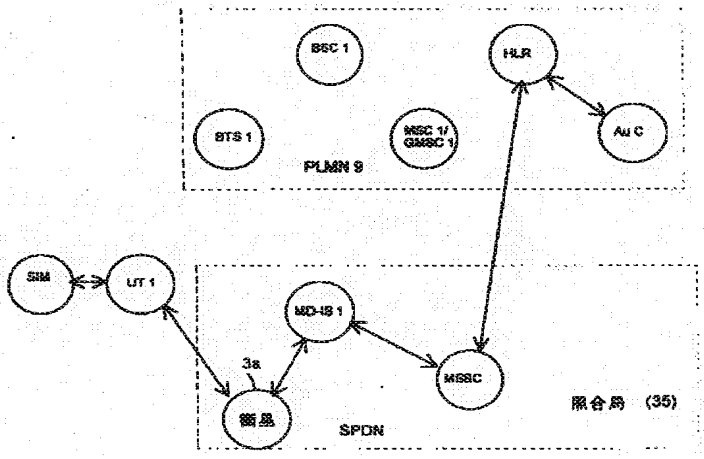
【図８】


BSC 1
HLR
BTS 1
MSC 1/
GMSC
Au C
PLMN 9
SIM
UT 1
MO-IS 1
3a
NASS
照合局 (35)
端末
SPDN

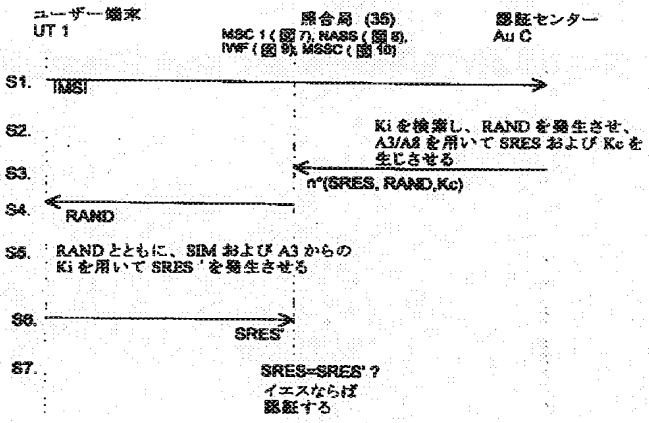
【図９】


BSC 1
HLR
BTS 1
MSC 1/
GMSC 1
Au C
PLMN 9
SIM
UT 1
MD-IS 1
3a
IWF
照合局 (35)
SPDN

【図１０】


BSC 1
HLR
BTS 1
MSC 1/
GMSC 1
Au C
PLMN 9
SIM
UT 1
MD-IS 1
3a
MSSC
照合局 (35)
SPDN

【図１１】


ユーザー端末
UT 1
照合局 (35)
MSC 1 (図 7), RASS (図 8),
IWF (図 9), MSSC (図 10)
認証センター
Au C
S1.
IMSI
S2.
Ki を検索し、RAND を発生させ、
A3/A8 を用いて SRES および Kc を
生じさせる
S3.
n*(SRES, RAND,Kc)
S4.
RAND
S5.
RAND とともに、SIM および A3 からの
Ki を用いて SRES ' を発生させる
S6.
SRES'
S7.
SRES=SRES' ?
イエスならば
認証する

CLAIMS

[Claim(s)]
[Claim 1]It is the method of attesting a move user terminal for use using the 1st or 2nd mobile network that supplies a service area to a common area, Each identification code by which said user terminal was held in this user terminal, In order to search authentication data corresponding to said identification code which could operate according to performs authentication using a corresponding identification code held in a remote authentication center set up beforehand, and was stored in said user terminal, Said authentication center is accessed through one as which it was chosen of said networks, An authentication method of a move user terminal including attesting said user terminal using said searched authentication data and data from said user terminal for said selected network from said authentication center.
[Claim 2]A method according to claim 1, wherein said 1st network supports transmission of a signal in the 1st mode and said 2nd network supports transmission of a signal in the 2nd mode.
[Claim 3]A method according to claim 2, wherein a signal in said 1st mode includes a voice channel signal and a signal in said 2nd mode includes a digital packet data signal.
[Claim 4]A method according to any one of claims 1 to 3, wherein said 1st network is a satellite long distance communication network and the 2nd network is PLMN.
[Claim 5]It is the method of attesting a move user terminal for use using the 1st mobile network, Said user terminal can operate using said 1st network and the 2nd network that supplies a service area to a common area, And use performs authentication beforehand set up for this user terminal, and said performs authentication, Each identification code held in said user terminal and a corresponding

identification code held in a memory site of said 2nd network are used, In order to search authentication data corresponding to said identification code held in said memory site in said 2nd network, Said 2nd network is accessed from said 1st network, An authentication method of a move user terminal including attesting said user terminal in said 1st network using said authentication data searched from said 2nd network, and data from said moving terminal.

[Claim 6]A method according to claim 5, wherein said 1st network is a satellite long distance communication network and said 2nd network is PLMN.

[Claim 7]It is the method of attesting a move user terminal for use using digital packet data networks, Said user terminal can operate to the voice channel communication in a mobile network using performs authentication to which it was beforehand set for a voice channel, and said performs authentication, Each identification code held in said move user terminal and a corresponding identification code held in a memory site in a network which supplies said voice channel are used, In order to search authentication data corresponding to said identification code stored in said memory site in said mobile network which supplies said voice channel, From said digital packet data networks, said mobile network which supplies said voice channel is accessed, An authentication method of a move user terminal including attesting said user terminal in said digital packet data networks using said searched authentication data and data from said moving terminal from said mobile network.

[Claim 8]A method according to claim 7, wherein said digital packet data networks use a satellite communication link to said move user terminal and said voice channel is supplied by public mobile network which puts a base station on the ground.

[Claim 9]A method comprising according to claim 7 or 8:

Identification data corresponding to said identification code stored in said user terminal is transmitted to said digital packet data networks from said terminal.

Said authentication data is transmitted to an authentication center in said voice network from said digital packet data networks.

According to said identification data, said authentication data is pulled out from said authentication center.

In order that said terminal may determine whether to be usable or not on said digital packet data networks, data pulled out from said terminal according to said appeal is compared [calling to said moving terminal about data corresponding to authentication data, and] with said authentication data.

[Claim 10]A method comprising according to claim 9:

Said authentication data is transmitted to collation positions in said digital packet data networks.
In said collation positions, said data pulled out from said terminal according to said appeal is compared with said authentication data.

[Claim 11]A method according to claim 9 or 10, wherein said moving terminal stores an identification code and each discriminant function of said each and said authentication center also contains said identification code and said each discriminant function further.
[Claim 12]According to performs authentication using each identification code held in a user terminal set up beforehand, for communication with a move user terminal which can operate, At least a part of 1st and 2nd mobile networks that supply a service area to a common area. In order to search an authentication center containing authentication data corresponding to said identification code stored in said user terminal, and said authentication data corresponding to said identification code, A transmitting means which transmits data from said user terminal corresponding to said identification code to said authentication center from said the 2nd either said 1st network or network, A long distance communications system including an authentication means which attests said user terminal using said searched authentication data and data from said user terminal for said selected network from said authentication center.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about attestation (authenticating) of the move (mobile) user terminal for one or more long distance communication networks, And it has the application to the satellite long distance communication network for supplying a long distance communication service area (coverage) to a move user terminal like a mobile phone handset (handsets) which is not characteristic, however restrictive.
[0002]

[Description of the Prior Art]The terrestrial move long distance communications system is known well, and various systems which operate by many various standards have developed. These public ground mobile networks (public land mobile networks:PLMNs) can operate by the analog or a digital standard. In the Far East except Europe and Japan, and other countries. To the digital global system mobile (Global System Mobile:GSM) network gaining popularity, in the U.S. The advanced type cellular system (Advanced Mobile Phone System:AMPS) and the digital type U.S. cellular system (Digital American Mobile Phone System:DAMPS) are used, Furthermore, the personal handy phone system (Personal Handiphone System:PHS) and the digital cellular communication system (Personal DigitalCellular:PDC) network are used in Japan. These days, the general move long distance communications system (Universal Mobile Telecommunications System:UMTS) is proposed more. All of these networks are cellular phone methods, and they place a base station on the ground (land-based).

[0003]For example, considering a GSM system, each cell (cell) of the mobile network is supplied by the ground base transmitter-receiver office (base transceiver stations:BTSs) estranged geographically [of a series].

This BTSs is connected with the mobile change center (mobile switching centre:MSC) through the base station change center (base switching centres:BSCs), This MSC can supply a gateway from a network to the conventional public change telephone network (public switched telephone network:PSTN).

Said network contains the home location register (home location register:HLR) which stores the information about the member and its user terminal to a system. When switch one of the user terminal is carried out, this user terminal is registered into HLR, and procedure of attestation is performed. The smart card known as Subscriber Identity Module (subscriber identification module:SIM) is supplied to each move user terminal, and this smart card stores two original discernment items, in order to identify a member. The 1st item comprises an international mobile subscriber identifier (international mobile subscriber identity:IMSI), and the 2nd item comprises a secret parameter mentioned as Ki in the specification of GSM. The authentication center (authentication centre:AuC) is connected with HLR.

The data corresponding to IMSI and Ki for each network member is included.

When switch one of the user terminal is carried out, and when it is others, IMSI is transmitted to HLR from a user terminal, and in order to attest a user, thereby, it refers for HLR to AuC. IMSI is compared in the memory of AuC and the value of corresponding Ki is searched. The random number RAND is generated within AuC. The

value of these random numbers RAND and Ki is applied as input data to the algorithm mentioned as A3 in a GSM specification, in order for a result with numerals (signed result) to generate SRES. AuC is further mentioned as A8 in a GSM specification, and this secret key Kc is used also including the algorithm which generates the secret key (secret key) Kc for the data encryption/decryption by which air transmission was carried out between the user terminal and the network which puts a base station on the ground. Actually, said algorithm A3 / A8 may be constituted by the single algorithm which makes 96 bit outputs from which 32 bits constitutes SRES and remaining 64 bits constitutes Kc generate. The signal of 3 groups which comprise RAND, SRES, and Kc is supplied to MSC through AuC to HLR, and this MSC acts as a collation office in performs authentication.

[0004]And the value of each RAND is transmitted to a user terminal through a network from MSC. SIM of a user terminal has algorithm A3 / A8 stored locally so that the value of corresponding SRES' and Kc may be generated in a user terminal from the value of the received random number RAND, and the value of Ki stored in SIM.

[0005]The value of SRES' is replied to MSC through a network and compared with the value of SRES generated at the beginning. When these are the same, a user terminal is attested, but the registration to HLR of a user terminal is prevented.

[0006]Then, if a user terminal is attested, MSC will start the data encryption/decryption transmitted through the network using the algorithm of the encryption/decryption mentioned as A5 in a GSM specification. The secret key Kc and the frame number of the data transmitted through the network are used for this A5 as the input. SIM of a user terminal generates the value of the secret key Kc of itself using the copy of the algorithm A8 stored locally. Thereby, the value of local Kc in a user terminal can be used in order to encipher / decipher the transmitted data using the copy of algorithm A5 held locally.

[0007]The advantage that only a random number is transmitted is among the performs authentication used by GSM with the air interface between a user terminal and BTS, and this makes danger of unjust registration the minimum.

[0008]About the further details of performs authentication, and the data encryption/decryption which continues after that. Refer to "The GSM System for Mobile Communications" (M. Mouly & M-B.Pautet, Cell & Sys.1992 pp 477-492).

[0009]When a user terminal moves to the GSM network with which geographically different places differ, a user terminal, Registering with the visitor position resistor (visitor location register:VLR) of the network of a visiting place, this VLR communicates with HLR which is a home network for bill creation dispatch and the

other purposes. DAMPS, PHS, and a PDC network also contain the similar position resistor.

[0010]Although the conventional analog PLMNs has supported service of digital packet data, transmission and reception of the message of a move user terminal, a facsimile, or E-mail are possible using this. For example, the AMPS network can support a cellular digital packet data (Cellular Digital Packet Data:CDPD) protocol, It becomes possible to transmit a data packet between the breaks of voice transmission with this protocol. About more detailed explanation of a CDPD system. Refer to "Cellular Digital Packet Data" (M. Streetharan and R.Kumar, Artech House Publishers, 1996 (ISBN-0-89006-709-0)). However, DAMPS and present digital PLMNs like GSM have covered the disadvantage of not supporting such digital packet data services.

[0011]

[Problem(s) to be Solved by the Invention]The move long distance communications system using a satellite communication link has been proposed between a move user terminal and a conventional ground network like PSTNs or PLMNs. Although one network known as IRIDIUM (trademark) satellite cellular system is indicated by the European patent laying-open-of-application No. 0365885 gazette and the U.S. Pat. No. 5,394,561 specification (Motorola), This uses the so-called conformation (constellation) of a low orbital circumference (low earth orbit:LEO) satellite, and these satellites have an orbital radius of 780 km. The link to the satellite on which an orbit is drawn high up in the air is established, and a telephone call is transmitted to other satellites in said conformation from this satellite, and a move user terminal like the handset of a telephone may usually be transmitted to the ground station connected with the network which establishes a base station in the conventional ground.

[0012]Other plans to use the so-called conformation of a middle earth orbit circumference (medium earth orbit:MEO) satellite are proposed with the orbital radius of the range of 10,000-20,000 km. About this. Walker J.G."Satellite. Refer to Patterns for Continuous Multiple Whole Earth Coverage" (Royal Aircraft Establishment, pp 119-122 (1977)). For example, refer to the ICO (trademark) satellite cellular system currently explained in the British patent application public presentation No. 2,295,296 gazette, and the ODYSSEY (trademark) satellite cellular system currently explained in the European patent laying-open-of-application No. 0,510,789 gazette. In these systems, a satellite communication link does not permit communication between adjoining satellites, but instead, the signal from a move user terminal like a move handset, It is first transmitted to a satellite, and is transmitted to a ground station or a satellite access node (satellite access node:SAN), and is connected to the telephone

network which establishes a base station in the conventional ground. There is an advantage that there are known digital ground cellular art and compatibility many whose components of a system are in this. [like GSM] It is also possible to use satellite communication art simpler than the case of a LEO network.

[0013]In the satellite communication network, the ground station is installed in various places in the world, in order to communicate with the satellite which draws and turns around an orbit. in an ICO (trademark) system and others, the visitor position resistor is connected with each satellite ground stations, and the satellite ground stations of each this hold record of each user terminal using a specific ground station. In order that a satellite communication network may enable E-mail, fax, and transmission of other data, the proposal that a digital satellite packet data network (satellite packet data network:SPDN) should be supplied is made. For example, the ICO (trademark) system is designed support such a packet data network.

[0014]The service areas supplied by conventional ground PLMN and satellite network in the area with the world will overlap in a common area. The proposal that each moving terminal operates on the both sides of PLMN and a satellite network is made. A user terminal may also include the switch which makes it possible to make a user choose a network, or auto select may be made again based on the intensity of a signal, for example. It is usually expected that the conventional ground network is liked for the reason of expense or signal strength. However, for a certain PLMN, if a certain service is supplied through a satellite network for a user terminal and other services can be supplied through PLMN, it is convenient. For example, the network which establishes a base station in the digital grounds, such as GSM, Since digital packet data services are not supported in present, in order to use the network of the digital packet data supplied by the satellite network to data transmission, it is convenient if a satellite network is used as extension of PLMN.

[0015]This invention enables voice channel communication to carry out through one long distance communication network like digital PLMN for example, And digital packet data communication relates to the attestation of a user terminal for operation with one or more networks so that it may become possible to carry out through other networks like a satellite network.

[0016]

[Means for Solving the Problem]Generally, this invention provides an authentication method of a move user terminal for using it in the 1st or 2nd mobile network that supplies a service area to a common area for communication by a user terminal. In this method, the user terminal could operate according to performs authentication set

up beforehand, and this performs authentication uses each identification code held in a user terminal, and a corresponding identification code held in a remote authentication center. In order to search authentication data corresponding to an identification code stored in a user terminal, this method, It consists of attesting a user terminal to a selected network using accessing an authentication center through one selected network, and authentication data and data from a user terminal which were searched from an authentication center.

[0017]The 2nd network is able for the 1st network to support transmission of a signal in the 1st mode like an audio signal, and to support transmission of a signal in the 2nd mode like a digital packet data signal.

[0018]Furthermore, a long distance communications system also provides this invention, and this long distance communications system, According to performs authentication using each identification code held in a user terminal set up beforehand, for communication by a move user terminal which can operate, The 1st and 2nd mobile networks that supply a service area to a common area, In order to search an authentication center containing authentication data corresponding to an identification code stored in a user terminal, and authentication data corresponding to an identification code, A means to transmit data from a user terminal corresponding to an identification code to said authentication center from either the 1st network or the 2nd network, A means which attests a user terminal for a network chosen from an authentication center using authentication data and data from a user terminal which were searched is included.

[0019]Furthermore, this invention also provides a method of attesting user–terminal communication in the 1st mobile network. In this method, performs authentication which could operate in the 2nd mobile network that supplies a service area which overlaps the 1st network, and was beforehand set up for a user terminal is used for a user terminal. This performs authentication uses each identification code held in a user terminal, and a corresponding identification code held in a memory site of the 2nd network. In order to search authentication data corresponding to an identification code held in said memory site of the 2nd network, said method, It consists of attesting a user terminal in the 1st network using accessing the 2nd network from the 1st network, and authentication data and data from a moving terminal which were searched from the 2nd network.

[0020]The 1st network may comprise a satellite long distance communication network, and the 2nd network may comprise PLMN.

[0021]This invention may use performs authentication for voice networks, in order to

attest communication which lets digital packet data networks pass.
[0022]This invention a move user terminal more specifically including a method of attesting for use which used digital packet data networks there, The user terminal can operate to the voice channel communication which used a mobile network, and this mobile network, This procedure uses each identification code held in a moving terminal, and a corresponding identification code held in a memory site of a network which supplies a voice channel using performs authentication beforehand set up for a voice channel. In order to search authentication data corresponding to an identification code stored in said memory site of a mobile network which supplies a voice channel, said method, A mobile network which supplies a voice channel is accessed from digital packet data networks, It consists of attesting a user terminal in digital packet data networks using authentication data and data from a moving terminal which were searched from a mobile network.
[0023]Digital packet data networks may use a satellite communication link to a move user terminal, and a voice channel may be further supplied by a public mobile network like a GSM network which puts a base station on the ground, for example.
[0024]A method by this invention transmits identification data corresponding to an identification code held at a user terminal from a terminal to digital packet data networks, Authentication data is transmitted to an authentication center in a voice network from digital packet data networks, According to identification data, authentication data is pulled out from an authentication center, It may include asking for data corresponding to authentication data, and calling to a moving terminal, and comparing with authentication data data pulled out from a terminal according to appeal, in order that a terminal may determine whether to be usable or not on digital packet data networks.
[0025]
[Embodiment of the Invention]Since this invention is understood more nearly thoroughly, the example which referred to the accompanying drawing explains this embodiment below. Drawing 1 is a schematic diagram showing the satellite long distance communications system by this invention with the local move long distance communications system which places a base station on the ground. Drawing 2 is a more detailed block diagram of an about one SAN satellite network and the ground cellular system network relevant to it, and is for showing a mutual operation. Drawing 3 is a rough block diagram showing the two-way communication in a satellite network. Drawing 4 is a schematic diagram of a move user terminal. Drawing 5 is a rough block diagram of the circuit of the terminal shown by drawing 4. Drawing 6 is a rough block

diagram of the SIM card shown by drawing 4 and drawing 5. Drawing 7 is a schematic diagram of the data flow relevant to attestation of GSM and PLMN9. Drawing 8 is a schematic diagram of a 1st embodiment of the performs authentication for SPDN. Drawing 9 is a schematic diagram of a 2nd embodiment of the performs authentication for SPDN. Drawing 10 is a schematic diagram of a 3rd embodiment of the performs authentication for SPDN. Drawing 11 shows roughly the data transmission between various components in the network for performs authentication.

[0026]* Reference of satellite network drawing 1 shows generally the rough block diagram of the satellite move long distance communications system corresponding to ICO (trademark). Move user-terminal UT1 of the form of a mobile phone handset can communicate through the radio channel of the communication paths 1 and 2 which went via the earth-orbit satellite 3a using satellite access node SAN1 which puts a base station on the ground. The antenna 4 which can pursue an orbital satellite is supplied to SAN1 as roughly shown in drawing 1.

[0027]It is connected and both much satellite access node SANS1, and 2 and 3 form the backbone network 5, and this backbone network 5 lets much Gateway G W1, and 2 and 3 pass, and is connected with the telephone network which establishes a base station in the conventional ground. For example, considering Gateway G W1, GW1 is connected with the public change telephone network (PSTN) 6 which places a base station on the ground, and this PSTN6 enables connection with the conventional telephone 7. Gateway G W1 is further connected to the public change data networks (PSDN) 8 and the public local mobile network (PLMN) 9. Each Gateway G W1, and 2 and 3 may comprise a mobile change center (MSC) which can obtain commercially form in which it is used in the GSM network.

[0028]As shown in drawing 1, handset UT1 can also communicate by mobile network PLMN9 which establishes a base station in the conventional ground, and this PLMN9 is roughly shown that it includes the transmitter-receiver office 10 which establishes the link 11 of the simultaneous-transmission-and-reception method of user-terminal UT1. In this example, PLMN9 is a GSM network. . Are published by the Europe long distance communication standard association (European Telecommunications Standard Institute:ETSI) for the more perfect understanding of GSM. Refer to various GSM advice (GSM Recommendations). Refer to above-mentioned "The GSM System for Mobile Communications" (M. Mouly & M-B.Pautet) as an outline which can be understood more easily.

[0029]Although the satellite network is designed supply a global service area and the satellites 3a and 3b form a part of conformation of a satellite, this satellite may be

arranged at some orbits. In one example, what has arranged five satellites which may be shown that it supplies the service area of most surface of the earth into two orbits is used. To the ascending vertical angle of the satellite of 10 degrees, one satellite can access all the time by a move handset, and two satellites can access at least 80% of time, and, thereby, supply the diversity of a system there. In order to supply redundancy (redundancy) and diversity furthermore, the satellite of further a long distance may be included in conformation.

[0030]Although a satellite is usually arranged, for example with the orbital radius of 10,355 km in MEO conformation, this invention is not restricted to a specific orbital radius. According to this embodiment, the satellites 3a and 3b are shown in a common orbit, and these satellites are pursued by the antenna arrangement of each SAN. Usually, each SAN contains five antennas, in order to pursue each satellite in conformation. In order to supply a service area without a break, SAN keeps an interval in terrestrial everywhere and is arranged. In the shown example, SAN1 may be installed in Europe, SAN2 may be installed in Africa, SAN3 may be installed in the U.S., and other SAN may be installed in other areas. It is shown by drawing 1 that SAN2 is communicating with user-terminal UT2 via the satellite 3b. Refer to the British patent application public presentation No. 2,295,296 gazette for the further details of a satellite network.

[0031]The satellites 3a and 3b may also include the feature which is in a non-geostationary orbit, and comprises a conventional satellite like fuse (Hughes) HS601 generally, and was indicated by the British patent application public presentation No. 2,288,913 gazette. Since the satellites 3a and 3b generate the arrangement of the beam which has covered the terrestrial electric wave receivable region of the satellite lower part, respectively, they are arranged, and each beam, The frequency channel and time slot from which a large number which are indicated by the British patent application public presentation No. 2,293,725 gazette differed are included. In this way, these beams supply adjoining cellular area and this cellular area supports the cell of the mobile phone network which establishes a base station in the conventional ground. Said satellite The satellite control center (satellite control centre:SSC) 12, It is controlled by pursuit telemetering and the control station (tracking telemetry and control station:TT&C) 13, This SSC12 and TT&C13 let the digital network 15 connected with the backbone network 5 pass, and are connected with the network management center 14. Although SSC12 and TT&C13 control operation of the satellites 3a and 3b, it is for, for example, setting up input tuning of a transmitting power level or a transponder, as transmitted in NMC14. It is received by

TT&C13, and the signal of telemetering for the satellites 3a and 3b is processed by SSC12, and ensures that these satellites function normally.

[0032]Handset UT 1 and 2 communicates with the satellites 3a and 3b between telebriefs via the channel of the perfect simultaneous-transmission-and-reception method which comprises a downlink channel and an uplink channel. Said channel contains a TDMA time slot on the frequency assigned on the occasion of a call start. A satellite link can be used for voice communication and further. For example, to the facsimile between a user terminal and SAN, a text message, E-mail, or other packet data transmission, it is a data rate of the range of 2.4-64k bps, and it is also possible to use for satellite digital packet data communication. Thus, the satellite network is supporting the satellite digital packet network (satellite digital packet network:SPDN).

[0033]Reference of drawing 2 shows the composition of SAN1 and local PLMN9 more to details. SAN1 consists of ground station LES1 connected with five sets of the dish type antennas 4 for satellite tracking, and this LES1 includes the amplifier, the multiplexer, the demultiplexer, and the transmitter-receiver circuit that has codec (codecs).Moving satellite change center MSSC1 is connected with LES1 and satellite visitor position resistor $VLR_{SAT}1$. MSSC1 makes signal transmission (a sound and packet data) connect with the backbone network 5 and LES1, and it lets the communication links 1 and 2 of the simultaneous-transmission-and-reception type which went via the backbone network 5 and the satellite 3a pass, It makes it possible to establish each telebrief to move user-terminal UT1. MSSC1 transmits a signal appropriately to those destinations according to the address on the signal transmission which enters from the antenna 4.

[0034]$VLR_{SAT}1$ holds IMSI of each user-terminal UT which uses SAN1 for each member's record, i.e., signal communication.

[0035]In order to control the flow of the packet data signal of the circumference of SPDN, mobile data relay station MD-IS is provided in each SAN so that SAN1 of drawing 2 may be shown. The overall flow of the digital packet data in a satellite network is controlled by network administrator (administrator) NASS, and this NASS may be installed with sufficient convenience in NMC14, as shown in drawing 1.

[0036]It is connected to Gateway G W1, and MSSC1 supplies output connection with PSDN8 and PSTN6 which were shown in drawing 1 also to PLMN9. In this way, packet data will usually be exchanged with PSDN8 and an audio signal will be exchanged with PLMN9 or PSTN6. In order to hold a registered subscriber's record, it turns out that all the SAN has each VLR_{SAT} and a similar structure.

[0037]If drawing 3 is referred to, the satellite network also contains the database 17

mentioned in this sentence as a satellite home location register (HLR_{SAT}) including the record relevant to each move user–terminal UT. Said record so that it may be explained in detail as the identifier of a terminal, i.e., the IMSI, by the present state of this UT, i.e., the following, It says [whether it is being operated in the "overall (global)" mode whether it is operating in the "local (local)" mode], Working SAN in which this UT is communicating with the geographical position of this UT and home MSSC into which this UT is registered so that bill record and other data can be collected at a single point via a satellite by this is included now. HLR_{SAT}17 may be installed in NMC14 shown in drawing 1, or may be distributed between SAN 1, 2, and 3 etc.

[0038]Reference of drawing 1 may register UT1 into one of the following two separate states. So that the "local" state where it is permitted that two separate states communicate only by UT's letting a part of one local area or satellite network pass, and UT may provide the use in a large area, It is in the "overall" state where the qualification for communicating through all the portions of a satellite mobile network is given.

[0039]* GSM network (PLMN9)

If drawing 2 is referred to again, the GSM mobile network 9 is the method by which this BTS is well known in itself including transmitter–receiver office BTS1 which establishes a base station in much grounds, 2, 3, etc., and in order to support a cellular system network, it is estranged geographically. Usually, the GSM network has a service area which laps on a country and states, and, so, overlaps the wide range service area of the satellite network. It turns out that BTS1 is shown with the connected antenna 10 and it is connected to base station change center BSC1 by the terrestrial communication line, and further two or more BTS(s) are the methods known well in itself, and are connected with BSC1. BSC1 is connected with mobile change center MSC1, and this MSC1, Within the limits of a mobile network, it is still more possible in a telephone call the conventional PSTN or to pass along Gateway G W1 via the wiring 19, and to transmit to a satellite network further, via the wiring 18 through Gateway G MSC1. Thus, a voice channel telephone call can be exchanged with UT1 through a GSM network. However, the GSM network is not supporting the digital transmitting and receiving packet data of user–terminal UT1.

[0040]The home location register HLR for GSM network 9 which puts a base station on the ground is connected with GMSC1, and is supplied. HLR holds record of IMSI of the user terminal registered for the use which used the network, and the details of the member relevant to this IMSI for the purpose of bill creation dispatch in the conventional method. Furthermore PLMN9 also contains the visitor position resistor

VLR, and this VLR moves from other GSM networks, and holds a member's record temporarily registered into the network. For example, when PLMN9 is put on Britain, the member from the GSM network of foreign countries, such as Germany, may be locally registered on a temporary base (basis), for example, while staying in Britain. The usage information of a telephone is relayed from VLR to a network of Germany for the purpose of bill creation dispatch via PSTN6 by the conventional method.

[0041]The authentication center AuC is connected with HLR. AuC contains the database and random number generator of Ki, and this database is uniquely connected with each member's IMSI with algorithm A3 / A8 according to GSM advice. This stored data is used in order to attest a user terminal like terminal UT1 so that it may explain to details more later.

[0042]* Reference of move user–terminal drawing 4 and drawing 5 designs move user–terminal UT1 operate in both a local ground cellular phone network and a satellite network. Therefore, in the example shown in drawing 2, it enables move handset UT1 to operate according to satellite either the GSM protocol which puts a base station on the ground or a network protocol. User–terminal UT1 comprises a move handset in which dual mode operation is possible as shown in drawing 4. The conventional GSM circuit for the use using the cellular system network 9 which puts a base station on the ground is included in this with the circuitry portion to which it was [for the use using a satellite network] similar. Handsets are the microphone 20, the loudspeaker 21, the battery 22, the keypad 23, the antenna 24, and a satellite link course, In order to display the message transmitted to the terminal through digital packet data networks, it comprises the display 25 which may be used for other component parts being mixed. Device UT1 which it can have by hand also contains the Subscriber Identity Module (SIM) smart card 26. The circuitry of handset UT1 is shown to drawing 5 by the block figure type. SIM card 26 is received in the SIM card reader 27 connected with the control device 28 which is usually a microprocessor. The microphone 20 and the loudspeaker 21 are connected with the codec 29, this codec 29 is connected with the conventional wireless interface 30 connected to the antenna 24, and signal transmission is transmitted and received [they are the method learned well thereby in itself, and].

[0043]As shown in drawing 6, SIM card 26 stores each IMSI including the memory M1 with algorithm A3/A8, and A5 by the discriminant function Ki with this memory M1 peculiar to SIM, and GSM advice.

[0044]* As the network selection above–mentioned was carried out, networks are many various methods and may be automatically chosen with either of the manual

types by factor like signal strength. In this example, a network is chosen as a manual type using the key on the keypad 23.

[0045]If the keypad 23 is operated in order to choose a satellite network, the control device 28 will operate so that the codec 29 and the wireless interface 30 may be constituted according to frequency, a protocol, and transmit frequency suitable for a satellite network. A voice transmission channel can be chosen as satellite networks. For example, digital packet data services can be chosen through SPDN according to the CDPD protocol used until now in a U.S. AMPS network. In this way, selection of a satellite network will perform both a voice channel and packet data communication via the satellite 3a through the simultaneous-transmission-and-reception method links 1 and 2.

[0046]If PLMN9 (GSM network) is chosen, the control device 28 will set up the wireless interface 30 operate through the simultaneous-transmission-and-reception method link 11 on frequency suitable for the GSM network voice channel which puts a base station on the ground. However, the GSM network cannot support digital packet data services by itself.

[0047]* When network interaction re-****2 is referred to, a satellite network, It may comprise an ICO (trademark) system, and every time this ICO (trademark) system lets the cellular system network which establishes a base station in the conventional GSM network 9 or other grounds pass, it can supply the enhanced service which cannot be used. In this example, the GSM network 9 cannot support PDN by itself. So, in a certain environment, it is desirable to transmit a telephone call through a satellite network from the mobile network 9 which puts a base station on the ground by that cause, and to use additional available service through a satellite network, using a satellite network as extension of PLMN9. The interaction-functions device 31 is supplied for this purpose, perfect control of the service facilities between the networks which establish a base station in a satellite and the ground of a cellular communication system is enabled, and it is using a satellite network by this, It makes it possible to support the packet data services of E-mail and others with a GSM network.

[0048]* As the performs authentication above-mentioned was carried out, when switch one of user-terminal UT1 is carried out, it is necessary to register with the network which should be used for the communication purpose, and performs authentication needs to be performed in order to determine the justification of a user terminal. Although the conventional GSM registration and performs authentication are performed to a GSM network (PLMN9), this is explained more to details with reference

to drawing 7 and drawing 11 after this.

[0049]According to this invention, for the use using the satellite packet data network SPDN of this conventional GSM registration procedure, It is evaluated that it is possible for it to be also adapted so that attestation of a user terminal may be supplied, with reference to drawing 8, drawing 9, and drawing 10, three examples about how performs authentication is used via SPDN are connected to drawing 11 there, and it explains them. GSM registration and performs authentication are first explained with reference to drawing 7.

[0050]1. GSM network (PLMN9)

As mentioned above, user-terminal UT1 contains the SIM smart card, and this SIM card stores only IMSI, the only discriminant function Ki, and GSM encryption algorithm A5 according to GSM advice (drawing 6). Registration and performs authentication are provided with the following.

IMSI is transmitted to the GSM attestation center AuC.

The data from SIM is compared with the data from the authentication center AuC in the collation office 35.

In the conventional GSM performs authentication, the collation office 35 is arranged in the GSM network, and may be arranged MSC1.

[0051]Drawing 7 shows the data flow between various components of a GSM network, and user-terminal UT1. The step of performs authentication is stated to drawing 11.

[0052]In the 1st step S1, it is transmitted to HLR from UT1 via BTS1, BSC1, and MSC1, and IMSI is transmitted to the authentication center AuC from there. As mentioned above, the authentication center AuC includes the copy of the discriminant function Ki relevant to each IMSI applicable to the use on a GSM network.

[0053]IMSI is compared within the memory of AuC and the value of corresponding Ki is searched with Step S2. The random number RAND is generated within AuC using a random number generator (not shown). Within AuC, the value of the random numbers RAND and Ki is applied as an input to a GSM algorithm, in order for a result with numerals to generate SRES. This secret key Kc is used also including the GSM algorithm A8 with which AuC generates the secret key Kc for the encryption/decryption of data by which air transmission was carried out between the user terminal and the network which puts a base station on the ground. Actually, algorithm A3 / A8 may consist of single algorithms which make 96 bit outputs from which 32 bits constitutes SRES and remaining 64 bits constitutes Kc generate.

[0054]In Step S3, the signal of 3 groups which consist of RAND, SRES, and Kc is supplied to MSC through HLR from the authentication center AuC, and this MSC

functions as the collation office 35 in performs authentication. Actually, although n 3 group signals are supplied during a telephone call to MSC for the use in just next attestation, in order to explain briefly here, 3 groups will consider only one processing, for example.

[0055]In step S4, the value of each RAND is transmitted to a user terminal through a network from MSC. The value of corresponding SRES' occurs in user-terminal UT1 from the value of Ki which SIM of user-terminal UT1 stored algorithm A3 / A8, and was stored in the received random number values RAND and SIM in Step S5 by this.

[0056]In Step S6, the value of SRES' is replied to MSC through a network and compared with the value of SRES generated at the beginning in Step S7. When these are the same, a user terminal is attested, but the registration to HLR of a user terminal is prevented.

[0057]When attestation is successful, MSC begins and the data encryption/decryption transmitted through the network using the algorithm mentioned as A5 in the GSM specification this A5, As the input, the frame number of the secret key Kc and the data transmitted through the network is used. Encryption and decryption are actually performed in BSC or BTS. SIM of user-terminal UT1 generates the value of the secret key Kc of itself using the copy of the algorithm A8 stored locally. In this way, the local value of Kc in user-terminal UT1 may be used in order to encipher / decipher data using the copy of algorithm A5 held locally.

[0058]Although only an essential random number is transmitted through an air interface, it turns out that these random numbers are mutually unrelated and danger of the use which is not reproduced and attested is made into the minimum.

[0059]According to this invention, it has been evaluated that it is also possible to use in order that this general art may attest SPDN so that it may explain below.

[0060]2. Attestation 2.1 of satellite digital packet network With reference to the 1st embodiment drawing 8 and drawing 11, the data flow for attestation of SPDN is explained below. Performs authentication uses the value which was held in IMSI from SIM, and AuC of GSM network PLMN9 and in which Ki was stored. Although the step of procedure is the same as that of what was generally shown in drawing 11, the collation office 35 comprises NASS in this case.

[0061]That user-terminal UT1 should be attested in Step S1 for the use which used SPDN IMSI, Although transmitted to PLMN9 via GW1 (drawing 1) via NASS (connected with NMC14) via the satellite 3a and MD-IS1 (connected with SAN1), IMSI is further transmitted to HLR and AuC as roughly shown in drawing 8. And at Step S2, IMSI is compared within the memory of AuC, and if just, the value of corresponding Ki

will be pulled out from a memory, as explained with reference to drawing 7. The value of each RAND is generated, algorithm A3 / A8 operate to RAND and Ki, and SRES and Kc are made to generate.

[0062]And in Step S3, 3 groups of SRES, Kc, and RAND are transmitted from AuC to the collation office 35, i.e., NASS.

[0063]In step S4, the value of each RAND passes along a network, is replied to user-terminal UT1 via satellite 3a, and as the value of corresponding SRES' mentioned above with reference to drawing 7 at Step S5 there, it is generated. In Step S6, in order to compare with the value of SRES in 3 groups received from HLR of PLMN9 before, the value of generated SRES' is replied to NASS via the satellite 3a and MD-IS1.

[0064]In Step S7, the value of SRES and SRES' is compared, and if they are the same, a user terminal will be attested for the use which used SPDN.

[0065]In this way, the procedure explained with reference to drawing 7 and drawing 8, Make it possible to attest a user terminal selectively because of either PLMN9 or SPDN, and by that cause a user terminal, It may be used for the packet data communication through the network SPDN which went via the object for voice communications and the satellite 3a on a GSM network, i.e., PLMN9.

[0066]When performs authentication is passed to other cells from the communication cell which has a system during transmission and 3 groups of other individuals (n-1) may be used for this purpose, it turns out that it may be repeated.

[0067]2.2 If the 2nd embodiment drawing 9 is referred to, the performs authentication shown in drawing 8 can be changed so that collation (Step S7) of SRES and SRES' may be performed by the interaction-functions device (interworking function unit) IWF shown in drawing 2. Therefore, IWF functions as the collation office 35. Drawing 9 shows the data flow for use by this embodiment. Although the value of SRES and the value of corresponding SRES' are generated by the same method as that (Step S1-S6) which was explained with reference to drawing 8, comparison (Step S7) of a signal value is performed by IWF.

[0068]2.3 Also in MSSC1 in suitable SAN (drawing 2), the function of the 3rd embodiment collation office 35 may be performed. Reference of drawing 10 shows the data flow to which it corresponds for performs authentication. The value of SRES and the value of corresponding SRES' are generated the same with having mentioned above, and are sent to MSSC1 for comparison, and this attests them for the use using SPDN of user-terminal UT1.

[0069]A terminal is attested by the authentication center (not shown) connected with

HLR_{SAT} shown in drawing 1, when communication of both a sound and packet data is thoroughly performed by the links 1 and 2 through a satellite network and PLMN9 is not chosen.

[0070]Many other corrections enter within the limits of this invention. For example, it turns out that PLMN9 can operate on the standard from which a large number, such as DCS1800 in PHS in Japan, PDC, or the countries of a certain Europe or newly proposed UMTS, differ, and a protocol.

[0071]Although this invention has been explained in relation to an ICO (trademark) satellite network, it can also use other satellite networks with various conformation and a signal transmission protocol.

[0072]Although the signal communication on the course 1 and 2 uses a TDMA access protocol, It is also possible to use other protocols like code division multiple access (code division multiple access) (CDMA) or Frequency Division Multiple Access (frequency division multiple access) (FDMA).

[0073]Since [of explanation] user–terminal UT is expressed for convenience, have used the word of "movement (mobile)", but. Or it can have this word in a hand, it should not be restricted to a portable terminal but, also including the terminal carried in a ship, an airplane, or vehicles on land for example, should be understood. It is also possible to fix a certain terminal UT selectively completely at least, and to carry out this invention.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a schematic diagram showing the satellite long distance communications system by this invention with the local move long distance communications system which places a base station on the ground.

[Drawing 2]It is a more detailed block diagram of an about one SAN satellite network and the ground cellular system network relevant to it, and is for showing a mutual operation.

[Drawing 3]It is a rough block diagram showing the two–way communication in a

satellite network.

[Drawing 4]It is a schematic diagram of a move user terminal.

[Drawing 5]It is a rough block diagram of the circuit of the terminal shown by drawing 4.

[Drawing 6]It is a rough block diagram of the SIM card shown by drawing 4 and drawing 5.

[Drawing 7]It is a schematic diagram of the data flow relevant to attestation of GSM and PLMN9.

[Drawing 8]It is a schematic diagram of a 1st embodiment of the performs authentication for SPDN.

[Drawing 9]It is a schematic diagram of a 2nd embodiment of the performs authentication for SPDN.

[Drawing 10]It is a schematic diagram of a 3rd embodiment of the performs authentication for SPDN.

[Drawing 11]The data transmission between various components in the network for performs authentication is shown roughly.

[Description of Notations]

UT1, UT2 user terminal

GW1, and 2 and 3 Gateway

1, 2, and 11 Simultaneous-transmission-and-reception method link

3a and 3b Satellite

4 Dish type antenna

5 Backbone network

6 PSTN

7 Telephone

8 PSDN

9 PLMN

10 Antenna

12 SCC

13 TC&C

14 NMC

15 Digital network

17 Database

18 and 19 Wiring

20 Microphone

21 Loudspeaker

22 Battery
23 Keypad
24 Antenna
25 Display
26 SIM smart card
27 SIM card reader
28 Control device
29 Codec
30 Wireless interface
31 Interaction-functions device (IWF)
35 Collation office
Reference number F05017A1

[Translation done.]